

技术要求与服务内容

1. 总则

1.1 本文档所指供应商、原厂商、乙方均为与甲方签订本项目采购合同的投标人，即：本项目中标人/中选乙方。本文档所指甲方、农行、我行、行内均为中国农业银行股份有限公司，即：本项目招标人/采购人。

1.2 除有特别说明外，本项目技术与服务要求均为关键性条款，即“刚性条款”，乙方应完全满足。如不满足，乙方响应将被视为不合格响应而被拒绝。如某条要求为非必须满足的，则该条要求前面将标注“非*”或“非刚性条款”。除有特别说明外，“刚性条款”中标记为“交付阶段满足”的需求均要求在交付时具备，未标记为“交付阶段满足”的需求要求在投标时具备。

1.3 在本项目合同履行期间，乙方派出的项目现场服务人员应为乙方（含其分公司、全资控股子公司、全资控股子公司下属分公司、全资控股子公司的全资控股子公司）或乙方母公司建立合法劳动合同关系的人员。

2. 项目背景情况说明

2.1.业务背景

在客户经理使用企业微信 APP 和客户个人微信 APP 聊天过程中，可能产生涉黄、涉恐、涉政等违法文字、图片、语音、视频等内容，计划采购内容质检工具，用于对企微相关业务场景的各种复杂内容进行质检。

2.2.建设目标及规划

为能够快速有效识别企业微信 1 对 1 聊天、对客群聊场景的各类风险，确保客户经理合规使用企业微信开展线上经营，本项目拟采购企业微信多种聊天场景的文本、图片、语音、视频等质检能力的质检工具，实现对企微海量多样聊天数据的合规质检，提升企业微信系统的风险防控能力。

3. 项目采购内容

序号	采购标的名称	主要功能模块/子系统/服务内容 (如有, 可选)	数量	使用范围	部署地点	备注 (服务期限、性能要求等其他需要特别说明的事项)	最高限价(不含税) (万元)
1	内容质检引擎软件(含 3	1. 内容质检服务模块, 针对文本、图像、音频、点/直播	场地内不	农银集团(含农业	数据中心(上海)/数据中心	场地内不限量使用授权 指在农银集团内(含甲方	358.41

	年免费维保)	视频等类型的内容,提供全方位的审核能力,覆盖涉黄、恐、暴、政、违规等违法、违规和有害信息等审核维度。 2. 内容质检管理模块,提供可视化、自定义的质检场景配置功能,包括选择审核模型、配置模型阈值实现松紧度调整、配置自定义敏感词表和人脸库等功能。 3. 维保主要包含远程技术支持、定期巡检、故障处理、定期软件升级等服务。	限量使用授权	银行境内外各级机构、控股子公司)	北京/数据中心 内蒙古/研发中心/一级分行	境内外分支机构、控股子公司)不受安装设备种类和数量限制,不受部署地点、部署方式及部署数量限制,不受注册用户和并发用户限制使用。	
2	内容质检引擎软件兼容性适配性改造 (含3年免费维保)	1. 主要包括与农行星云、交付中心、USAP等相关系统对接以及农行基础软硬件适配等。 2. 维保主要包含远程技术支持、定期巡检、故障处理、定期软件升级等服务。	场地内不限量使用授权	农银集团 (含农业银行境内外各级机构、控股子公司)	数据中心(上海)/数据中心 北京/数据中心 内蒙古/研发中心/一级分行	场地内不限量使用授权 指在农银集团内(含甲方境内外分支机构、控股子公司)不受安装设备种类和数量限制,不受部署地点、部署方式及部署数量限制,不受注册用户和并发用户限制使用。	66.98

4. 知识产权要求

1. 所购软件产品目标码及知识产权要求: 乙方向甲方(农行,下同)提供可执行程序目标码(目标码定义为可执行程序), 甲方自交货之日起享有所购产品非独占的永久使用权, 甲方可在农银集团内(含甲方境内外分支机构、控股子公司)不受安装设备种类和数量限制, 不受部署地点、部署方式及部署数量限制, 不受注册用户和并发用户限制使用。

2. 兼容性适配性改造部分开发成果: 甲方有权对所购软件产品进行兼容性适配性改造开发。甲方拥有软件产品兼容性适配性改造部分的全部知识产权及源代码所有权。乙方交付给甲方该软件的兼容性适配性改造部分的源代码及其相关文档,所提供代码纳入甲方版本库进行管理。乙方应保证提供的所有代码符合甲方要求,具有规范性和可编译性。甲方享有软件产品兼容性适配性改造部分源码的使用权、修改权,可以根据甲方业务需求对软件产品兼容性适配性改造部分源代码进行代码检查、查看审计以及编译并生成可执行程序投入使用。

3. 乙方保证其根据本合同提供的软件及服务没有任何权利瑕疵,没有侵犯任何第三方权利,在实施本项目中使用的各种软硬件开发、维护工具软件拥有知识产权或者拥有权利人授权其使用并许可第三人使用的权利。甲方在使用该软件或服务的任何一部分时,免受第三方提出的侵犯其知识产权的权利主张。如果任何人对甲方使用该软件或服务主张权利,由乙方负责处理一切纠纷及相关事宜。由此给甲方造成的损失,由乙方承担,其承担范围包括赔偿费、诉讼费(仲裁费)等相关的费用。

4. 乙方在服务过程中接触和获取的甲方技术或者信息，不得对外泄露或者提供给他人使用，不得用于其他委托事项。

5. 软件产品需求说明

5.1 软件产品功能要求

5.1.1 功能概述

本项目软件产品，针对文本、图像、音频、点/直播视频等类型的内容，提供全方位的审核能力，覆盖涉黄、恐、暴、政、等违法、违规和有害信息等审核维度，同时提供可视化、自定义的质检场景配置功能，包括选择审核模型、配置模型阈值实现松紧度调整、配置自定义敏感词表和人脸库等功能，功能要求概述如下：

主要功能模块名称	实现功能简述
内容质检服务模块	针对文本、图像、音频、点/直播视频等类型的内容，提供全方位的审核能力，覆盖涉黄、恐、暴、政、等违法、违规和有害信息等审核维度。
内容质检管理模块	提供可视化、自定义的质检场景配置功能，包括选择审核模型、配置模型阈值实现松紧度调整、配置自定义敏感词表和人脸库等功能，以及系统管理和运维管理功能。

5.1.2 内容质检服务模块

内容质检服务模块，针对文本、图像、音频、点/直播视频等类型的内容，提供全方位的审核能力，覆盖涉黄、恐、暴、政、等违法、违规和有害信息等审核维度。

内容质检服务模块要求支持内容形式主要包括文字、图片、音频、视频，内容质检服务模块要求识别多种违法、违规和有害风险类型，包括涉黄、涉政、暴恐、违禁、谩骂、违规广告、敏感及价值观等，具体的功能要求如下：

内容形式	功能需求	需求描述	备注
文本	支持语言	支持检测汉语（简体中文和繁体中文）	
		支持检测英语	非刚性条款
		支持检测藏语	非刚性条款
		支持检测维语	非刚性条款
	支持格式	支持主流文本字符编码类型，包括 UTF-8，GBK、ANSI 等编码。	

	支持长度	支持检测不超过 5000 字符的文本	
		支持检测大于 5000 字符的文本	
	支持接口	支持开放 RESTful HTTP API 接口	
	支持反馈	支持反馈合规与否的检测结果，支持反馈不合规标签	
	支持的检测分类	支持涉政质检	
		支持涉黄质检	
		支持暴恐质检	
		支持违禁质检	
		支持谩骂质检	
		支持广告质检	
		支持价值观质检	
图片	支持格式	支持主流图片类型，包括 jpg、jpeg、png、gif 等。	
	支持大小	支持检测 10MB 及以下的图片	
		支持压缩 10MB 以上超大的图片并进行检测	
	支持接口	支持开放 RESTful HTTP API 接口	
	支持反馈	支持反馈合规与否的检测结果，支持反馈不合规标签	
	支持的检测分类	支持图片中的文本质检	
		支持涉政质检	
		支持涉黄质检	
		支持暴恐质检	
		支持违禁质检	
		支持广告质检	
		支持恶心类质检	
音频	支持格式	支持主流音频类型，包括 WAV、MP3、WMA、AMR、FLAC、APE、ALAC、WavPack 等；支持格式：支持 HTTP、MRCP、websocket 传输协议，实时语音封装格式支持包括 WAV、MP3、ACC、AMR、Speex 等，音频编码格式支持包括 MP3、ACC、AMR、Speex、G. 711、G. 729、G. 722、G. 722. 1、G. 722. 1C 等	
	支持长度	支持检测 60 分钟及以内的音	

		频	
		支持对超过 60 分钟的音频进行分片检测	
	支持接口	支持开放 RESTful HTTP API 接口	
	支持反馈	支持反馈合规与否的检测结果，支持反馈不合规标签，支持反馈不合规音频的位置	
	支持的检测分类	支持音频转文本内容质检	
		支持人物声纹质检	
		支持涉黄质检	
		支持引人不适声音质检	
视频	支持格式	点播方面，支持 HTTP 传输协议，支持主流点播视频文件类型，包括 MP4、AVI、MOV、WMV、RM、RMVB、MPEG、WMF 等传输协议，视频编码格式支持 h264，h265，av1 等	
		直播方面，支持 RTMP/HTTP 传输协议，直播视频封装格式支持 MP4，FLV，MPEG-TS，视频的编码格式支持 h264，h265，av1 等	
	支持长度	支持检测 5GB 及以内的视频文件	
	支持长度	支持对流式的视频检测（或是分割视频片段）进行检测	
	支持接口	支持开放 RESTful HTTP API 接口	
	支持反馈	支持反馈合规与否的检测结果，支持反馈不合规标签，支持反馈不合规视频的位置，不合规类型（画面不合规还是音频不合规）	
	支持的检测分类	支持视频中文本台词质检	
		支持视频中音频质检	
		支持视频截帧图片质检	
		支持视频行为模式质检	非刚性条款

所有违法、违规和有害风险信息识别模型的 F1 值达到 0.85（含）以上。（质检模型评价数据：

(1) TP（True Positive）：预测为违规、违法和有害信息内容条数，实际为违规、违法和有害信息内容条数；

- (2) FP (False Positive)：预测为违规、违法和有害信息内容条数，实际为正常的内容条数；
- (3) TN (True Negative)：预测为正常的内容条数，实际为正常的内容条数；
- (4) FN (False Negative)：预测为正常的内容条数，实际为违规、违法和有害信息内容条数。

内容质检引擎主要关注指标：

- (1) 准确率 (Accuracy, A)： $(TP+TN)/(TP+FP+FN+TN) \times 100\%$ ，对于给定的测试数据集，正确分类的样本数与总样本数之比。
- (2) 精确度 (Precision, P)： $TP/(TP+FP) \times 100\%$ ，识别出违规、违法和有害信息内容条数的精确程度；
- (3) 召回率 (Recall, R)： $TP/(TP+FN) \times 100\%$ ，识别到的违规、违法和有害信息内容条数占有“应该检索到的内容条数”的比例；
- (4) F1： $2*(P*R)/(P+R)$ ，综合评价质检模型的效果。

文本、图片、音频、视频等检测分类，要求必须能够识别下面表格中 85%以上的标签，即 88 个标签中至少识别 75 个（含）标签，其他单项要求参见下表备注列：

序号	内容形式	检测分类	标签	备注
1	文本	支持涉政质检	诋毁国内领导人	至少要识别 1 项标签
2			诋毁国外领导人	
3			诋毁英雄人物	
4			落马官员	
5			政治异见人士	
6			政治违禁作品	
7			反动分裂人物、组织及作品等	
8			邪教迷信人物、组织及作品等	
9			政治运动、敏感事件人物、组织及作品等	
10			民族宗教高敏内容	
11			群体社会事件	
12			国家机关、军警、会议、政策法规等谣言、负面内容	
13		支持涉黄质检	色情作品及资源	至少要识别 1 项标签
14			色情人物	
15			色情交友	
16			色情道具用品	
17			性器官描述	
18			淫秽语句/色情段子	
19			色情挑逗暗示	
20			儿童色情	
21		支持暴恐质检	暴恐人物、组织及作品等	至少要识别 1 项标签
22			暴恐事件	
23			暴力犯罪及恐怖作品及资源	
24			暴力犯罪及恐怖描述	

25			武器制作及资源	
26		支持违禁质检	赌博&高利贷	至少要识别 1 项标签
27			违禁毒品、药品和化学品	
28			管制刀具、监控设备、翻墙工具等违禁物品/工具	
29			非法服务，包括且不限于造假、代开发票、代刻公章、考试论文枪手、私家侦探等	
30			代孕捐精	
31			人口&器官买卖	
32			侵犯个人隐私的信息	
33			疑似涉诈风险	
34			劣迹艺人等违禁人物和作品	
35		支持谩骂质检	人身攻击类侮辱谩骂	至少要识别 1 项标签
36			粗言秽语	
37			地域、性别、人种等歧视诋毁	
38		支持广告质检	电商微商推广、引流等	至少要识别 1 项标签
39			企业推广、引流等	
40			违规兼职、违规代理	
41			金融投资等高危广告	
42			医院、培训机构等广告	
43			灌水无意义内容	
44			广告法限制的内容	
45		支持涉价值观质检	反动价值观内容	至少要识别 1 项标签
46			历史虚无主义	
47			有违道德伦理	
48			封建迷信	
49			拜金炫富	
50			美化涉黑犯罪	
51			不利未成年健康成长	
52		支持其他违规质检	其他违法、违规及有害内容	
53	图片	支持图片中文本内容质检	图片文本内容质检	要求识别
54		支持涉政质检	政治人物违规图像，包括诋毁&影射领导人、英雄人物，反面人物等	至少要识别 1 项标签
55			反动分裂组织旗帜、标志和宣传物	
56			邪教迷信组织旗帜、标志和宣传物	
57			敏感或负面的国内外事件场景	
58			群体社会事件场景	
59			不规范的地图	
60			涉政封禁的作品、logo、标识	

61		支持涉黄质检	色情人物	至少要识别 1 项标签
62			器官、物品及行为等色情内容	
63			裸露、暗示等低俗内容	
64			卡通色情图片	
65			儿童色情图片	
66		支持暴恐质检	暴恐人物	至少要识别 1 项标签
67			暴恐事件场景	
68			纳粹、暴恐组织旗帜、标识和宣传物	
69			暴恐服饰	
70			暴力犯罪场景	
71			恐怖图片	
72		支持违禁质检	违禁行为图片，包括且不限于赌博、吸毒、吸烟、饮酒、竖中指等	至少要识别 1 项标签
73			违禁物品图片，包括且不限于管制刀具、武器、毒品、药品、钱币等	
74			劣迹艺人	
75			违禁场景图片，包括且不限于封建迷信、恐怖灵异场景	
76		支持广告质检	识别广告二维码、小程序码，识别二维码的内容	要求识别
77		支持恶心类质检	引起大多数人生理、心理强烈不适的图片，包括血腥、排泄物、脏器等场景	要求识别
78		支持其他违规质检	其他违法、违规及有害图片	
79	音频	支持音频转文本内容质检	音频转文本内容质检	要求识别
80		支持人物声纹质检	包括领导人、反动分裂组织人物、邪教迷信组织人物声纹	要求识别
81		支持涉黄质检	娇喘、呻吟等色情挑逗声音	要求识别
82		支持引人不适声音质检	高分贝噪声、ASMR 等给人造成生理、心理不适的声音	要求识别
83		支持其他违规质检	其他违法、违规及有害的声音	
84	视频	支持视频中文本台词质检	提取视频中台词文本质检	要求识别
85		支持视频中音频质检	提取视频中音频内容质检	要求识别
86		支持视频截帧图片质检	视频文件、直播拉流抽帧切片为图片质检	要求识别
87		支持视频行为模式质检	对视频中色情、暴恐、违禁等动作行为质检	
88		支持其他违规质检	其他违法、违规及有害的视频	

		检		
--	--	---	--	--

5.1.3 内容质检管理模块

5.1.3.1 质检场景管理功能

内容质检管理模块-质检场景管理功能主要提供质检业务配置管理相关能力，包括：

1. 质检场景管理：新建、查询、修改和删除质检场景，包括质检场景包括消费方渠道，选择质检模型（配置支持的内容形式和风险类型），配置自定义敏感词表和敏感人脸库等。
2. 质检模型列表管理：按照质检场景维度，对选择的质检模型列表进行增、删、改、查操作。
3. 质检模型参数管理：按照质检场景维度，为质检模型配置不同阈值参数，从而质检松紧度调整。
4. 敏感词表管理：按照质检场景维度，对自定义的敏感词表进行增、删、改、查操作。支持配置不少于 1000 个敏感词，敏感词配置后要在 10 分钟内生效。
5. 敏感人脸库管理：按照质检场景维度，对自定义的敏感人脸库进行增、删、改、查操作。敏感人脸库配置的图片，支持 jpg、jpeg、png、gif 格式，支持配置不少于 1000 个敏感人脸图片，敏感人脸配置后要在 10 分钟内生效。
6. （非刚性条款）自定义质检规则管理：支持对接行内私有化大模型服务，利用大模型能力开展自定义规则质检。

5.1.3.2 系统管理功能

内容质检管理模块-系统管理功能主要提供系统运营相关能力，包括：

1. 权限控制：支持对用户、角色、菜单等进行权限控制调整。
2. 流量统计：统计系统总体访问情况，各接口访问情况。
3. 系统接口管理：管理后台提供接口级访问控制，能控制接口是否可用。
4. （非刚性条款）流量控制：管理后台系统可监控网关流量，支持配置上下游流量阈值及并发连接阈值。
5. （非刚性条款）服务熔断：提供切实可行的服务熔断/恢复功能。

5.1.3.3 运维管理功能

内容质检管理模块-运维管理功能主要提供系统运维相关能力，包括：

1. 日志管理：日志记录，日志查询和日志导出，包括管理模块登录、操作日志，以及服务模块系统运行日志。
2. 系统运行数据监控：对质检请求数据进行监控，包括达到和处理时间，并识别出异常情况。
3. （非刚性条款）统计报表，按照日期、内容形式、风险类别、有害信息识别率、质检场景等维度监控并统计系统运行情况。

5.2 软件产品非功能性要求

5.2.1 性能效率

需求类别	需求描述
用户数量	管理端软件支持的总用户数量 1000、平均在线数量 10、峰值在线用户数量 200
联机响应时间	单实例最大的资源数 144C384G, 8 张 T4 情况下, 服务模块响应时间: 文本质检联机响应时间小于等于 800ms (长度 5000 字符以内), 图片质检联机响应时间小于等于 2000ms (图片在 10MB 以内), 音频质检联机响应时间至少支持 1: 10 (60 秒以内音频, 每秒处理 10 秒音频), 视频质检联机响应时间至少支持 1:4 (60 秒以内, 每秒处理 4 秒视频); 管理模块响应时间: 500ms。
批量处理 (异步处理)	单实例最大的资源数 144C384G, 8 张 T4 情况下, 文本每秒处理不少于 10000 字, 图片每秒处理 10MB 图片 1 张, 音频质检至少支持 1:10 (每秒处理 10 秒音频), 视频质检至少支持 1:4 (每秒处理 4 秒视频);
吞吐量	单实例最大的资源数 144C384G, 8 张 T4 情况下, 文本不低于 100QPS (长度 5000 字符以内), 图片不低于 5QPS (图片在 10MB 以内), 音频至少支持 10 路并发 (60 秒以内音频), 视频至少支持 5 路并发 (60 秒以内视频), 直播流不低于 5 路并发。
网络带宽	支持在千兆以太网运行
主机交易部署	不涉及
会话管理	应用服务器与数据库服务器之间会话连接支持异常重连机制 (当数据库切换或重启后, 应用服务器支持重连)
其他	无

5.2.2 兼容性

需求类别	需求点	需求描述
操作系统兼容性 (交付阶段满足)	服务器端	软件服务器端应支持我行 CCE 云上环境欧拉 V2.9 操作系统及版本, 其中内容质检管理模块与服务模块分开部署的产品, 内容质检管理模块应支持我行 CCE 云上环境麒麟 V10 操作系统及版本, 且能够满足行内要求, 后续 (产品交付时) 内容质检管理模块与服务模块均支持我行 CCE 云上环境麒麟 V10 操作系统及版本。
	用户 PC 客户端	不涉及
	用户移动终端	不涉及
浏览器兼容性	Web 访问支持	软件应支持用户通过 web 方式访问。
	PC 端 web 访问	应支持 IE、Edge 浏览器, 兼容 Chromium 内核的浏览器及版本。
	移动端 web 访问	不涉及。

	问	
基础软硬件兼容性（交付阶段满足）	服务器端、桌面端基础软硬件	软件应支持、兼容、适配我行确定的以下服务端、桌面端基础软硬件，并能跟随以下基础软硬件的升级而同步升级。我行服务端、桌面端基础软硬件具体要求如下： 1. 服务端： 运行使用环境：我行 CCE 云上环境； 服务器：Intel（X86 架构）服务器类型，其中内容质检管理模块与服务模块分开部署的产品，内容质检管理模块支持海光（X86 架构）服务器或鲲鹏（ARM 架构）服务器；后续根据行内要求全部适配支持海光（X86 架构）服务器或鲲鹏（ARM 架构）服务器； GPU：Nvidia T4，后续根据行内要求适配其他 GPU。 服务器操作系统：欧拉 V2.9，其中内容质检管理模块与服务模块分开部署的产品，内容质检管理模块应支持麒麟 V10，后续根据行内要求全部适配支持麒麟 V10； 数据库：软件运行如果依赖数据库，需兼容行内 TDSQL、Redis； 中间件：软件运行如果依赖 web 中间件，需兼容行内 Tomcat，其中内容质检管理模块与服务模块分开部署的产品，内容质检管理模块支持 TongWeb； 其他：软件运行如果依赖大数据组件，需兼容行内 kafka、zookeeper、ElasticSearch； 2. 桌面端： 浏览器：支持 IE、Edge 浏览器，兼容 Chromium 内核浏览器； 桌面操作系统：支持 windows、linux、Uos。 3. 其他：无。
	基础桌面软件	不涉及。
注：软件在正式交付前，如我行需要更换调整软件运行支持、兼容、适配的服务端、桌面端基础软硬件、基础桌面软件，更换后的软硬件不在上述所列示的支持、兼容、适配的软硬件清单内，需要乙方对其产品进行适配改造的，乙方应予以免费支持。		

5.2.3 易用性（交付阶段满足）

需求类别	需求描述
在线帮助	提供服务调用 API 文档，提供详细的在线/离线操作手册等
容错响应	单机服务出现超时后，应及时向星云监控平台反馈故障原因，并通过降级、熔断机制、集群高可用等方式保证服务对外正常运转
用户个性化	针对不同的用户、用户组定义人员，提供可配置化管理功能
UI\UE 原型	符合我行 UI/UE 要求规范，包括浏览器端及移动端 Logo、UI/UE 设计、登录页面、首页面本地化等，并且保证易用性

5.2.4 可靠性（交付阶段满足）

需求类别	需求描述
灾备等级	要求支持私有云部署，系统支持异地灾备或双活或两地三中心部署。
应用系统可用性	全年 7*24 小时不间断运行，应支持负载均衡，系统运维时间 18:00-24:00，0:00-8:30
外部系统容错性	外部系统故障恢复时，系统对外服务、状态监控等应可以自动恢复
基础软件容错	基础软件故障恢复时，系统对外服务、状态监控等应可以自动恢复
数据丢失处理机制	应支持数据刷新或重构等措施解决数据丢失或错误问题

5.2.5 可维护性（交付阶段满足）

需求类别	需求描述
系统调试	应用系统内部的调试语句在生产版本时应进行控制，支持调试日志输出；发现问题需要跟踪程序时，支持通过日志跟踪生产运行状态
应用替换	在应用系统替换过程中，支持与原来的软件同时工作，避免所有节点停止导致服务中断，系统升级应保证向前兼容
参数配置	支持界面化参数配置，配置参数存储方式等
批量作业调度	应用系统的批量作业调度和操作作业集中调度平台(简称BJS)进行统一的批量作业调度和批量作业操作等
监控	系统接入我行星云智能运维平台-监控中心实现告警覆盖 系统监控须覆盖以下指标（交易量、平均响应时间、成功率）
批量监控	应用系统批量运行时按照 BJS 监控
日志	系统必须接入实现应用日志统一采集、查询、分析的功能，系统具备运行日志和错误日志记录功能；同时系统需支持对管理员的操作行为进行记录，形成操作行为日志；日志中涉及的敏感信息需进行脱敏处理。
操作	系统必须接入星云智能运维平台，实现应用所有分区的平台化可用性技术验证功能；系统必须接入星云智能运维平台，实现所有运维操作的平台化调度和实施，且必须包含应用启停场景；部署数据库的系统，必须接入星云智能运维平台-操作中心 数据操作，实现应用数据库数据的平台化查询和变更
交付	系统必须对接交付中心，实现应用系统的自动交付
分析	系统按需接入星云智能运维平台-分析中心，实现系统交易量自动采集

5.2.6 数据生命周期管理（交付阶段满足）

需求类别	需求描述
在线阶段	质检场景、模型阈值、敏感词表和敏感人脸库等配置数据支持永久存储，日志相关数据支持 60 天的存储
归档阶段	支持基于行内标准，将应用系统产生的全部数据归档保存
销毁阶段	系统功能支持归档数据销毁

5.2.7 质检敏感数据更新要求

（非刚性条款）乙方能够提供准实时（日频）更新敏感词库、敏感人脸库等数据的能力，支持主动推送或联机接口的方式进行同步更新。

5.3 软件产品安全要求

5.3.1 功能性安全要求

需求类别	需求描述
身份鉴别	提供专用的登录控制模块对登录用户进行身份标识和鉴别，接入行内 USAP 系统进行行内员工身份认证，采用用户密码认证+人脸识别或短信验证码进行双因素认证。
访问控制	1. 建立安全的访问控制机制，在用户未登录时不能直接访问相应资源。2. 采用最小授权等必要的访问控制模型，不同用户提供不同的权限，实现访问控制功能，控制用户对文件、数据库表等客体的访问。3. 提供会话超时机制，用户在长时间未使用系统时，系统自动断开登录，登录操作超时终止会话，再次接入必须强制重新登录。
信息展示	非明文显示用户输入的口令、用户使用完安全介质后，安全介质未取出时提供提示消息等。
安全审计	提供覆盖每个用户的安全审计功能，明确应用系统重要安全事件，并记录重要安全事件的审计日志等。
个人信息保护	采用加密措施实现用户信息的保密性；同时对敏感信息需进行脱敏展示；应提供隐私政策查询的入口，在服务器端记录用户对隐私政策的同意详情等
客户端安全	优先使用服务端数据，仅从前端获取必须由用户输入或选择的信息：1、用户登录或交易时获取用户的权限信息并缓存在应用服务端 session 中，具体包括 token 信息等，后续交易流程权限控制由服务端鉴权服务统一管控。2、对于多次前后交互类交易，每一步骤均应优先从后台获取业务数据。3、对于应用服务端返回客户端的业务数据，仅返回业务功能视角的最小必要数据，且仅用于前端显示，不再回传作为后续交易的输入。4、对于手工录入的数据，在应用服务端进行是否为空、类型、长度、范围、防越权的合法性校验，结合本条线数据模型形成统一的检查组件，通过切面统一检查。
输入与输出安全控制	明确合法数据格式和范围，对系统接收数据进行有效性验证。保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。限制用户上传文件的格式、大小，系统对用户上传/下载文档操作进行校验。
用户异常行为分析与风控	禁止用户越权访问、禁止客户端用户访问安全策略禁止的内容，记录用户操作行为，可查看分析用户异常操作。
业务安全	系统提供的报表设计功能需符合行内规范。
特定功能模块安全	图片验证码、短信、邮件、手势密码、手机指纹密码、手机人脸识别、生物识别通用等
数据安全	数据存储、使用、数据通信、行内用户数据等要求符合行内的相关数据安全

需求类别	需求描述
	全规范。配置文件中不能明文存放相关密码信息。
证书安全	在行内基础安全平台（UPKI）可支持托管的情况下，含私钥的第三方应用证书应托管到行内基础安全平台（UPKI），调用行内基础安全平台（UPKI）提供的通用安全服务。（注：可支持托管指的是证书格式为 pfx 格式或可改造成 pfx 格式）

5.3.2 安全资质认证要求

乙方应具备以下信息安全管理体制资质认证之一（资质认证要求从乙方投标阶段到产品维保服务有效期内均需具备）：

- ISO/IEC 27001（或 GB/T 22080）信息安全管理体制。
- ISO/IEC 20000 信息技术服务管理体制。
- ISO/IEC 22301 业务连续性管理体制。
- ISO/IEC 27701 隐私信息管理体制。
- ISO/IEC 27018 公有云中个人可识别信息管理体制。
- ISO/IEC 27017 云服务信息安全管理体制。

5.3.3 安全测评报告要求

产品在生产环境完成部署前，乙方需对其产品开展安全测评，并提供相应的测评报告。安全测评报告中的测评关注点宜涵盖组件安全、服务配置安全、会话安全、数据安全、通用漏洞防范、身份认证、业务逻辑安全、客户端安全、SDK 安全、隐私合规、安全审计、密码算法、代码安全等 13 类，具体可参考附件《安全测评要求及关注项清单》。

除上述对软件自身的安全测评报告外，结合该软件的内容质检功能和使用场景（对文字、图片、语音、视频进行检查），需在生产环境完成软件部署前取得中国信通院出具的内容审核服务系统测评相关类型的证书，并提供信通院的认证证书复印件。

5.3.4 第三方及开源基础软件/组件安全要求

交付软件或所交付软件版本升级时中如使用或更新了第三方及开源基础软件/组件，则乙方应对使用的第三方及开源基础软件/组件漏洞情况进行排查，并将第三方及开源基础软件/组件使用清单（开源软件名称、版本号、开源协议信息等）纳入交付物，排查结果应符合我行对开源软件安全的统一要求。乙方应加强对自身产品和所涉及的第三方及开源基础软件漏洞情报的监测，当发现自身产品或第三方或开源基础软件出现安全漏洞后提供必要的漏洞修复技术支持。

第三方及开源基础软件/组件漏洞排查结果及开源软件清单应纳入交付验收材料范围（模板见附件《第三方及开源组件清单、漏洞技术评估和协议合规审查情况说明》、《第三方及开源基础软件清单、漏洞技术评估和协议合规审查情况说明》）。

5.3.5 用户口令安全要求

为防范弱口令漏洞，乙方应提供全量的操作系统用户、中间件用户、应用系统预置用户和口令清单。

用户和口令清单纳入交付验收材料范围。

5.3.6 软件产品代码安全和漏洞修复要求

软件应不包括任何削弱应用安全性的代码，包括：已知漏洞，病毒，时间炸弹、后门、木马、复活节彩蛋，及所有其它形式的恶意代码。乙方应采用所有合理措施确保软件安全。

乙方应采用必要措施保护与我行供应链安全产品有关的源代码、配置文件、用户名口令、设计文档等敏感数据安全，及时发现并阻断源代码等敏感数据外泄渠道。不应使用互联网代码托管平台、互联网文档共享平台、乙方的外包服务商的代码管理平台等保管敏感数据。例如，不应使用 github、csdn、pudn 等平台进行源代码托管。若乙方发现软件产品疑似存在源代码等敏感数据泄露，应及时进行阻断并通知我行。

产品交付后以及维保期内，若我行发现新的软件漏洞，乙方需要在约定时间内做出响应，提供修复处置方案；若乙方发现新的软件漏洞，需要及时升级我行部署的产品，配合完成漏洞修复工作。

5.3.7 乙方网络安全相关责任和义务

1. 乙方应采取防范计算机病毒、网络攻击、网络侵入等危害网络安全行为的管理和技术措施，实时监控网络安全威胁，严格管控人员操作权限，保障自身网络设施安全。
2. 乙方应建立供应链产品（不含技术服务）全生命周期安全管控机制，加强研发过程中的需求架构管控和安全测试，以及发现产品漏洞后提供必要的漏洞修复技术支持。
3. 乙方应提升应急处置能力，针对不同类型和级别的网络安全事件制定应急响应方案并定期演练，应急响应方案应覆盖源代码泄露、供应链中断、漏洞修复等场景。
4. 乙方应承诺严禁私自开通远程运维，严禁基于任何目的私自预留后门或带有后门性质的功能。
5. 乙方应允许本行根据需要对其开展网络安全相关评估或检查。
6. 乙方应承诺加强威胁情报检测，及时将涉及本行供应链产品相关威胁情报及时告知本行，如发生网络安全事件须配合本行开展调查。
7. 乙方应采用可信或可控的产品分发、交付和仓储手段。

5.4 软件产品其他要求

5.4.1 软件产品许可要求

采购的应用软件使用范围应为农银集团（含农业银行境内外各级机构及控股子公司等），场地内不限量使用授权，场地内不限量使用授权指在农银集团内（含甲方境内外分支机构、控股子公司）不受安装设备种类和数量限制，不受部署地点、部署方式及部署数量限制，不受注册用户和并发用户限制使用。

5.4.2 软件产品部署实施要求

按照行内技术架构及部署架构要求，在支持 5.2.2 兼容性内容的基础上，在产品交付阶段提供私有云部署的部署方案。私有云部署方案应适配我行 CCE 环境，满足 CCE 的应用部署、资源管理等要求。此部分费用包含在报价中，不需要单独收费。

6. 软件兼容性适配性改造需求

乙方需要按照我行要求完成本章节的兼容性适配性改造任务和目标。我行将按照该章节的工作成果及工作质量要求进行验收评价。

6.1 兼容性适配性改造

6.1.1 兼容性适配性改造概述

本项目兼容性适配性改造要求概述如下：

主要兼容性适配性改造内容	实现功能简述
接入星云智能运维平台	实现系统监控、操作、交付和日志等运维分析功能
对接统一调度平台	实现批量作业的统一调度
对接文件管理平台	实现文件的存储和读取
对接统一安全认证平台	实现用户统一认证与鉴权
对接内容质检模型引擎前置服务	实现质检服务的提供
应用服务与管理配置分离	服务模块与管理模块打包部署的，支持将管理端进行拆分独立部署

6.1.2 接入星云智能运维平台

6.1.2.1 对接监控中心

接入星云智能运维平台-监控中心，进行服务状态的监控及告警，支持日志监控、联机监控、批量监控、网页监控等。按照场景、渠道、机构等维度实现交易量、平均响应时间、成功率等指标的监控。

6.1.2.2 对接操作中心

接入星云智能运维平台-操作中心：

1. 接入数据查询和数据变更模块，实现应用数据库数据的平台化查询、变更。
2. 接入应用验证模块，实现应用所有分区的平台化可用性技术验证，实现一键式应用整体可用性验证。
3. 接入应用操作模块，实现所有运维操作的平台化调度和实施，包括应用启停操作。

6.1.2.3 接入交付中心

接入星云智能运维平台-交付中心，实现程序平台化部署，支持部署流水线。

6.1.2.4 接入日志中心

接入星云智能运维平台-日志中心，对日志进行存储、监控、查询、分析等。

6.1.3 对接统一调度平台

对接统一调度平台，实现批量作业运行的远程集中调度和统一监控。

6.1.4 对接文件管理平台

对接文件管理平台，实现文件的存储、读取。

6.1.5 对接统一安全认证平台

对需要用户认证的功能，对接统一安全认证平台，提供密码、短信、电子令牌、指纹、数字证书、双因素认证等各级别认证服务和单点登录服务，并进行用户信息和认证凭证管理。同时，提供 OAuth 授权功能供接入系统使用。

6.1.6 对接内容质检模型引擎前置服务

采购的软件作为内容质检模型引擎的能力支撑模块，对接内容质检模型引擎前置服务，通过 API 和批量的方式提供质检服务。

6.1.7 应用服务与管理配置分离

在正式交付前，服务模块与管理模块打包部署的，支持将管理端进行拆分独立部署。

6.2 兼容性适配性改造部分非功能性以及安全要求

软件产品实现兼容性适配性改造后，兼容性适配性改造部分非功能性要求、安全要求与 5.2 章节软件产品非功能性要求、5.3 章节软件产品安全要求一致。

7. 项目实施需求说明

7.1 项目组织架构要求

为了明确项目兼容性适配性改造或定制化开发中，不同实施阶段甲乙双方的角色和责任，并有利于乙方评估工作量以给出合理报价，下表中给出了我行建议的责任分工。要求乙方据此进行项目计划编制、组织架构设置以及工作量评估。

工作阶段及任务		乙方	我行
项目管理		配合	负责
需求编写及产品设计（主要指兼容性适配性改造等内容）		共同负责	共同负责
开发测试	需求分析	共同负责	共同负责

阶段	设计与开发	负责	配合
	接口开发与联调	负责	配合
	集成测试	负责	配合
	系统测试	负责	配合
	业务验收测试	配合	负责
投产阶段	系统安装、部署	共同负责	共同负责
	系统投产上线	共同负责	共同负责
运行阶段	系统日常维保与技术支持	共同负责	共同负责
	版本升级	共同负责	共同负责

7.2 项目里程碑及实施进度要求

里程碑	标志性事件	交付物	预定时间（T+N，以合同签订当月作为T月）
兼容性适应性改造 功能需求编写	乙方按照对本需求书的应答，编写相关的需求规格说明书。	需求规格说明书	T+1
兼容性适应性改造 功能系统开发	乙方与我行分析需求，共同进行开发设计、接口联调，实现需求规格说明书所列软件功能。	按照 CMMI 要求 乙方出具各个阶段必须的文档。 包括系统设计文档等	T+4
兼容性适应性改造 功能系统测试和验收测试	测试交付	功能测试报告、性能测试报告、安全测评报告、信通院认证证书复印件、业务验收报告等	T+5
兼容性适应性改造 功能系统上线	系统开发测试完毕后，配合我行技术部门进行项目投产模拟演练，演练通过后按照农行业务管理规定，在规定时间内进行系统上线	操作手册、应急手册等	T+5
兼容性适应性改造	产品开发完成后，对我	1、完善、有效、	T+6

功能用户培训	行开发人员的进行系统使用技术培训；对总行运维人员进行系统运维技术培训	可操作的培训计划书 2、完整的系统使用技术培训书面教程及讲义 3、完整的系统运维技术培训书面教程及讲义 4、培训总结报告	
注：各里程碑完成时间以甲方阶段性项目实施计划为准。			

7.3 项目具体实施要求

7.3.1 项目测试要求

乙方将产品交付我行测试验证前，需完成内部系统测试，并向甲方测试部门交付测试方案、测试报告等文档。我行测试部门选取一定交易进行验证，未发现缺陷视为通过；若仍发现缺陷，需要乙方重新执行系统测试并交付，直到达到我行要求为止，对后续项目周期产生的影响由乙方承担。

乙方应根据我行要求，提供项目系统测试（包括自动化测试、安全测试、性能测试等）相关技术支持，保证软件能够按照我行要求的质量交付。

7.3.2 人员要求

农行对乙方团队成员要求如下：

工作时间要求：基于实施工作整体计划表开展工作，如需请假请提前 1 个工作日告知甲方；如需进入农行场地内工作，需遵循外部人员现场服务管理要求。

人员雇佣关系要求：乙方团队成员必须为乙方（含其分公司、全资控股子公司、全资控股子公司下属分公司、全资控股子公司的全资控股子公司）或乙方母公司建立合法劳动合同关系的正式员工。

人员资质要求：国家承认学历大学本科及本科以上学历，工作经验不少于 3 年，具备熟练的开发维护本软件产品所需的编程能力。

人员变更要求：乙方必须提供团队成员的完整个人材料，并经农行的确认后才能参加此项目，更换人员的资质水平不低于原团队成员。

乙方需保证主要成员的稳定。

7.3.3 系统投产要求

内容质检引擎系统投产上线工作由农行、乙方共同负责。上线准备期间，乙方承担的工作包含：系统测试环境安装与配置、系统兼容性适应性改造、与其相关部分的技术和业务培训等。

8. 维保服务要求

8.1 维保服务对象及起止时限

乙方提供本项目软件产品及兼容性适配性改造部分三年期维保服务，维保服务自软件产品及兼容性适配性改造部分全部验收完毕并稳定运行三个月，双方签署《软件产品稳定运行三个月阶段验收表》确定的验收合格之日起计算。

8.2 维保服务组织要求

本项目要求原厂等级的维保服务（此处原厂等级是在维保人员构成上，可按照 7.3.2 章节人员要求中的人员提供服务，且至少要包含 3 名原厂人员（指乙方人员）。另外，在人员的使用和管理等方面，乙方需要承担连带责任）。乙方应按照本项目的维保服务要求、服务水平和交付文档制定服务计划和方案并提供相应服务。

乙方应成立针对农行本项目维保服务的不少于 5 人的技术支持团队，团队成员要求要符合原厂等级的要求。技术支持团队主要负责本章节维保服务有关工作，及时处理各类故障并恢复系统正常运行。按照我行的要求，提交服务要求中的相关文档。维保团队组成人员须经过我行的审查认可。

8.3 维保服务内容及具体要求

8.3.1 远程技术服务要求

在维保期内，乙方须提供无限制的 7×24 小时电话和 Email 技术支持服务，对远程无法解决的问题须提供必要的现场技术支持，直至问题解决。乙方项目相关管理人员、技术工程师的电话要保持 24 小时开通，随时处理各种突发事件。

8.3.2 定期巡检服务要求

乙方每季度提供一次软件产品（含兼容性适配性改造部分）的巡检服务（巡检服务地点包括：数据中心（上海）/数据中心北京/数据中心内蒙古/研发中心/一级分行，具体巡检地点以行方实际要求为准），对系统运行环境进行健康检查，提出潜在问题解决方案，解决遗留的技术问题，并认真填写《维保服务定期巡检报告》，以保障系统安全、稳定、高效运行。

如因不可抗力等客观原因（如洪水、地震等自然灾害、疫情管控等）不能到达现场的，经双方协商与评估，在行内人员自行检查可安全实施且不影响检查质量的情况下，可采用乙方电话或视频等方式远程指导行内人员进行系统健康状况检查。该方式视同乙方已完成本次巡检工作（仍需出具巡检报告）。

8.3.3 故障处理服务要求

乙方提供 7×24 小时故障报修服务热线电话，当产品发生故障时，我行可以通过热线电话获得服务支持。乙方根据故障诊断结果，采取包括现场服务（现场服务地点包括：北京、上海、呼和浩特等）以及其它相应措施，确保最短时间内恢复产品正常使用。乙方应具有应

急处理流程，当现场工程师遇到不能按时解决的疑难问题时，能够得到有效的后援支持。现场故障处理结束后，填写《维保服务故障处理报告》。

乙方故障响应方式及时间按照故障级别要求如下：

故障等级	定义	要求响应方式
非常严重	1. 全部业务或关键业务受到灾难性影响； 2. 由于软件原因可能会对农行声誉造成重大影响的故障。	1. 维保人员 <u>10</u> 分钟内响应，并着手分析问题； 2. 维保人员在 <u>2</u> 小时内到达指定服务地点； 3. 提交应急恢复方案，确保在 <u>4</u> 小时内恢复业务正常开展； 4. 按 7×24 小时持续努力，至问题解决； 5. 进行问题根源性分析。
严重	1. 部分业务受严重影响； 2. 服务严重受损或严重降级。	1. 维保人员 <u>10</u> 分钟内响应，并着手分析问题； 2. 维保人员在 <u>2</u> 小时内到达指定服务地点； 3. 提交应急恢复方案，确保在 <u>6</u> 小时内恢复业务正常开展； 4. 按 7×24 小时持续努力，至问题解决。 5. 进行问题根源性分析。
一般	1. 服务中度受损或中度降级，在受影响的情况下工作仍能合理继续； 2. 只对极小部分客户/用户产生影响的故障。	1. 维保人员 <u>30</u> 分钟内响应，并着手分析问题； 2. 在保障不影响系统或业务运行的前提下，24 小时内视情况派驻现场维保人员并解决系统故障； 3. 提交恢复方案， <u>8</u> 小时内恢复业务正常开展； 4. 进行问题根源性分析。
较小	1. 业务受最小程度的影响； 2. 实质上正常进行，对服务仅造成微小障碍或无障碍。	1. 维保人员 60 分钟内响应，并着手分析问题； 2. 提交恢复方案，24 小时内恢复业务正常开展。

注：

- 1、故障等级要以我行工程师判断级别为准，具体故障级别定义参考上表。
- 2、响应时间，指在所选择服务等级允许的服务时间内接到故障电话起，乙方所能够提供的正确的故障判断或有效解决方案的时间。
- 3、人员到达现场时间，指乙方做出响应后派驻维护人员到达指定故障地点的时间。
- 4、系统恢复时间，指工程师到场后到系统恢复运行的时间。

8.3.4 升级服务要求

软件版本，是指当软件产品的内容或功能发生变化时，需要对软件产品进行升级，每次升级的软件产品通常为一个版本。根据与现版本软件内容或功能发生变化的大小程度，农业银行定义的外购软件产品升级版本分为补丁版本、小版本、大版本。农业银行外购软件产品的版本分类及具体定义如下：

版本分类	具体定义
补丁版本	产品相对现版本进行了局部细微修改或系统 bug 修正后的新版本。
小版本	产品进行了局部少量修改或在现版本产品基础上进行了局部功能优化调整，但新功能与现有功能差别不大。
大版本	产品进行了重大修改或局部修正累积较多，而导致产品整体发生了较大全局变

版本分类	具体定义
	化。
注： 1. 如乙方产品交付后，乙方在现有产品上新增研发了功能模块（或功能组件），且该新功能模块（或功能组件）与产品其他部分具有相对独立性，乙方针对该功能模块（或功能组件）对其已签订合同的所有客户均以新产品模块或组件形式进行增量销售，该功能模块（或功能组件）可视为不属于该产品大小版本升级服务范围。 2. 如乙方产品交付后，乙方对产品进行了重构，乙方针对新重构产品对其已签订合同的所有客户均以新产品进行销售，新重构产品可视为不属于该产品大小版本升级服务范围，但新重构产品主要是为解决现有产品无法修复的安全漏洞或缺陷的情况除外。新重构产品主要是为解决现有产品无法修复的安全漏洞或缺陷的，乙方应为甲方进行免费软件升级替换。	

1. 乙方应提供本次采购软件产品(含兼容性适配性改造部分)的补丁和大小版升级服务，并可根据甲方需要提供现场实施支持。具体包括：

- (1) 软件 bug 修正；
- (2) 软件安全漏洞、缺陷修复；
- (3) 乙方提起的软件补丁和大小版本升级；
- (4) 甲方系统的功能调整，但新交易与现有交易差别不大。
- (5) 其它升级内容，质检模型、敏感词表、敏感人脸库和敏感声纹库的更新升级，需支持每半年升级一次。

（非刚性条款）乙方能够提供准实时（日频）更新敏感词库、敏感人脸库等数据的能力，支持主动推送或联机接口的方式进行同步更新。

2. 乙方应及时将已知产品存在的安全漏洞、缺陷、bug 和产品升级要求等信息通知甲方，对于关键的补丁及升级版本，乙方应在其发布一周内制定相应的升级计划，通报我行相关部门及时升级。

3. 当软件在交付时支持、兼容、适配的我行服务端、桌面端基础软硬件、基础桌面软件进行版本升级时，乙方提供的软件产品应能够同步升级，并支持、兼容、适配我行升级后的服务端、桌面端基础软硬件、基础桌面软件。

4. 维保期内，当我行需要更换软件运行适配的服务端、桌面端基础软硬件、基础桌面软件时，如更换后的软硬件不在软件交付时应支持、兼容、适配的服务端、桌面端基础软硬件、基础桌面软件清单内，且乙方产品需进行较大修改调整或架构改造的，双方可另行协商改造方式及具体商务事宜。

5. 升级包必须来源于原厂商。

6. 乙方明确版本升级实施流程，并形成升级方案，制定有效的紧急情况处理流程和应急预案、提供升级介质和技术文档，经过甲方技术部门审核批准后实施，确保升级后的产品满足我行应用系统的需要。

7. 根据甲方需要，乙方在升级过程中，对系统测试的案例、自动化测试脚本应进行同步更新和维护，在升级完成后，乙方应对升级软件进行跟踪，提供升级结果测试等报告类文档提交我行保存。

8.3.5 特殊时点服务要求

因系统架构变更、应用调整、新业务上线投产等原因需要对该项目内维保产品进行变更操作时（包括安装、卸装、配置、调试等服务内容），以及农行业务应用重要时段（如重大节假日或重要活动期间、结息、年终决算等关键业务时段），乙方需根据我行需要派具有相关产品维保资历和经验的专业服务人员到现场实地操作或远程特护，保障系统的稳定运行。

8.4 维保服务其他要求

本合同约定的软件产品可在农银集团内不限部署数量且不限部署地点及方式使用，在产品维保期内，我行因业务发展需要、系统架构变更、应用调整、新业务上线投产等原因，在农行境内外分支机构或本合同约定使用范围内新增加或调整产品部署地点及数量的，新增加或调整后的产品应纳入本合同维保服务范围（维保服务要求与本合同一致），乙方在本合同维保期内不应再新增收取维保服务费用。

9. 培训及知识转移要求

9.1 培训服务要求

乙方需提供产品的技术和业务知识相关培训服务，详细课程要求如下：

培训课程 1: 系统使用培训

培训时间：3 天(每满 8 小时算 1 天)

培训地点及环境要求: 甲方场所

讲师资质要求：乙方精通系统研发使用的技术人员

培训内容、参加人数: 软件产品的工具使用、中间件使用、自动化测试、系统配置等使用方法，大于 5 人

培训教材及其他材料：系统使用技术培训书面教程及讲义

培训课程 2: 系统运维培训

培训时间：3 天(每满 8 小时算 1 天)

培训地点及环境要求: 甲方场所

讲师资质要求：乙方精通系统研发使用的技术人员

培训内容、参加人数: 软件产品的部署、升级、日志分析、故障排查、应急、出错处理、数据备份恢复等运维方法，大于 5 人

培训教材及其他材料：系统使用技术培训书面教程及讲义

9.2 知识转移要求

9.2.1 文档转移要求

乙方应按照甲方需要，及时向甲方转移软件产品与技术服务有关文档。文档主要包括以下内容（乙方根据甲方项目交付时的实际文档要求提供）：

设计文档、术语说明、命名规范、信息安全规范、应用接口规范等相关技术文档，单元测试报告、集成测试报告、系统测试报告、测试案例、自动化测试脚本、用户使用手册、系统安装手册、系统维护手册、系统应急操作手册等。

9.2.2 技能转移要求

乙方应根据甲方需要，通过培训以及其他乙方认为合适的方式实现业务、技术及应用维护、系统维护技能的转移，转移内容包含：软件开发生命周期方法、软件工程方法、开发语言及工具的使用、相关中间件的使用、定制化开发等，以及项目管理、整体实施架构设计、质量控制、集成测试、系统测试、自动化测试、数据迁移、用户验收测试、产品投产流程、日常运行维护、出错的处理及解决、数据备份与恢复等项目集成、实施、应用维护等方面的技能。

9.2.3 源码转移要求

对于兼容性适应性改造功能，要求乙方的所有开发代码需纳入我行版本库统一管理，且源代码安全水平符合我行标准要求，测试和投产环境的所有目标码需通过版本库统一生成并测试，经验收测试完成后的源码版本再执行上线流程。

10. 软件及服务验收

验收阶段	验收内容	交付物	验收内容
软件产品到货阶段	对软件产品功能、性能、介质、许可证等相关材料进行验收	介质（如有） 许可证文件（如有） 安全测评报告 信通院认证证书复印件 其他软件有关材料	详见附件：《软件产品到货阶段验收表》
兼容性适应性改造开发阶段	对阶段性研发目标进行考核验收	项目需求分析说明书 设计说明书 项目兼容性适应性改造源码	
试运行阶段	对试运行情况进行验收	试运行情况报告 应用系统配置说明书 操作手册 应急手册 开源软件漏洞排查结果和开源软件清单（如产品涉及） 用户和口令清单（如产品	详见附件：《稳定运行三个月阶段验收表》

		涉及)	
整体验收阶段	对项目整体服务质量进行考核验收	技术支持服务登记表(如有) 紧急现场服务报告(如有) 系统巡检服务报告 系统升级服务报告(如有)	详见附件:《维保阶段验收表》

各阶段验收结果分为合格、基本合格和不合格三类:

(一) 合格。标的物全部验收指标完全符合合同约定。

(二) 基本合格。标的物的关键核心验收指标完全符合合同约定, 非关键核心验收指标存在瑕疵但不影响标的物使用。

(三) 不合格。标的物全部验收指标低于合同约定, 或部分关键核心验收指标低于合同约定; 未列入验收内容但合同有约定的其他违约事项。

11. 合同款项支付

验收阶段	支付计划	支付金额
试运行阶段	软件及兼容性适配性改造上线并稳定运行三个月后支付合同主体款项	软件及兼容性适配性改造总金额的 90%
维保服务阶段	维保期满, 根据维保服务验收情况, 支付合同质量及服务保证金	软件及兼容性适配性改造总金额的 10%

甲方根据上述验收阶段验收结果支付相应阶段款项:

1. 验收结果为合格的, 全额支付相应阶段款项;
2. 验收结果为基本合格的, 甲方视乙方对其存在问题整改情况减值支付相应阶段款项, 并根据合同约定提供减值依据, 乙方应予接受;
3. 验收结果为不合格的, 原则上不支付合同相应阶段款项。若乙方整改后, 经甲方重新验收合格的, 应视为基本合格, 减值支付相应阶段款项。

12. 其他要求

12.1 技术服务保密协议要求

乙方应与我行签订技术服务保密协议。

12.2 外部服务人员要求

1. 合同签订后，乙方应提供为我行现场服务的人员名单（含身份证件信息）。乙方（含其分公司、全资控股子公司、全资控股子公司下属分公司、全资控股子公司的全资控股子公司，下同）及乙方母公司应与其公司的相应服务人员签署保密协议，对服务人员开展安全培训及合同约定服务所须遵守的本行规范的培训，对服务人员开展背景调查且经调查无不良行为记录。乙方及乙方母公司应出具《外部服务人员资质承诺函》。
2. 现场服务人员均需签署《外部人员安全承诺书》，乙方及乙方母公司组织其外部服务人员签署；乙方需保证承诺书均由与乙方建立合法劳动关系的员工签署，对其员工所签署的承诺书负责。使用乙方全资控股子公司、全资控股子公司下属分公司、全资控股子公司的全资控股子公司、乙方母公司提供服务的，乙方全资控股子公司、全资控股子公司下属分公司、全资控股子公司的全资控股子公司、乙方母公司需保证承诺书均由与其建立合法劳动关系的员工签署，对其员工所签署的承诺书负责。同时要求乙方作为采购合同的签署方，保证其对于相关表述或承诺承担连带责任。在协议履行期间，乙方及其母公司对其派出人员的安全负全部责任，负责办理必要的保险并支付相关保险费。如派出人员在协议履行中发生事故、意外的，乙方应负责处理并承担全部责任。甲方与乙方及其母公司派出的技术服务人员不构成劳务派遣关系。乙方及乙方母公司组织员工签署承诺书后，在外部人员首次入场提供现场服务时，统一将承诺书提交至甲方各外部人员使用需求部门。

12.3 网络安全审查要求

1. 乙方须承诺其所投产品不包含未通过国家网络安全审查或正在接受审查的产品或产品部件。
2. 乙方须遵守国家《网络安全审查办法》相关规定。
3. 根据国家《网络安全审查办法》要求，若经甲方预判为需要向国家网络安全审查办公室申报网络安全审查的产品或产品部件或服务，中标候选人/中标人有义务配合网络安全审查工作，所需申报材料应在接到甲方通知的10个工作日内提供，并不得利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不得中断产品供应或必要的技术支持服务。产品和服务通过网络安全审查后方可确定中标人，未通过网络安全审查的取消中标资格。中标候选人/中标人因未履行网络安全审查义务（包括但不限于不配合审查、故意隐瞒、提供虚假申报材料等）而造成甲方直接或间接损失的，甲方保留追究责任权利。
4. 因乙方产品不符合国家网络安全法律法规规定或合同履行过程中因乙方产品或服务原因造成甲方重大损失，甲方有权终止本合同，另行安排服务商，由此造成的损失由乙方承担。

12.4 续保价格约定

免费维保期满后，甲方有权决定是否需要从乙方继续购买相同标准的维护服务，如需要，则在保证维保要求不变的情况下，由乙方提供的软件及兼容性适配性改造部分维护服务每年费用（不含税）不超过本项目相应货物（即相应软件及兼容性适配性改造部分）价格（不含税）的10%，以采购结果为准。

12.5 测评要求

本项目将对投标产品进行技术测试，具体以测评方案为准。

12.6 退出情况

若出现产品不能满足国家网络安全要求或乙方网络安全责任落实不到位的情况，甲方有权终止合同，一切损失由乙方承担，具体情况包括但不限于：

1. 乙方提供的产品或服务存在重大安全隐患，导致本行蒙受重大经济损失，或造成重大网络安全事件的。
2. 乙方知而不报，或恶意植入木马、病毒等，导致本行蒙受重大经济损失，或造成重大网络安全事件的。
3. 乙方存在违法违规行为的，包括但不限于未经授权违规数据收集、滥用大数据分析、非法远程接入等行为的。
4. 经评估其产品不满足国家网络安全法律法规要求的乙方。
5. 国家或监管禁止使用或不推荐使用的信息化产品和服务。

12.7 需明确的其他要求

乙方自行承担到达甲方的交通费用，以及在甲方研发场地发生的必要费用（例如交通、住宿、餐饮）等。

附件：维保服务定期巡检报告

[illegible]

注：本表格一式两份，甲乙双方各执一份，作为服务评价依据。

附件：维保服务故障处理报告

项目（合同）名称			
合同编号			
我行主管部门		乙方公司名称	
我行现场负责人		乙方现场工程师	
我行联系电话		乙方联系电话	
故 障 日 期		故障现场地点	
故障现象与处理			
故障发现时间		故障发现人	
故障响应时间		响应工程师	
工程师到场时间及人员名单			
备件到场时间及数量型号描述			
故障最终解决时间			
故障现象描述：			
故障分析与处理结果：			
我行现场负责人签名：_____ 乙方现场工程师签名：_____ 日 期：_____ 日 期：_____			

注：本表格一式两份，甲乙双方各执一份，作为服务评价依据

附件：升级服务报告

项目（合同）名称			
合同编号			
我行主管部门		乙方公司名称	
我行现场负责人		乙方现场工程师	
我行联系电话		乙方联系电话	
升 级 日 期		升级完成时间	
工程师到场时间及人员名单			
升级类型	☐ 大版本 ☐ 小版本 ☐ 补丁更新、缺陷修复 ☐ 安全漏洞修复 ☐ 其他：		
升级具体内容及过程描述： 升级结果：			
我行现场负责人签名：_____ 乙方现场工程师签名：_____			
日 期：_____ 日 期：_____			

注：本表格一式两份，甲乙双方各执一份，作为服务评价依据。

附件：安全测评类要求及关注项清单

安全测评类建议包括组件安全、服务配置安全、会话安全、数据安全、通用漏洞防范、身份认证、业务逻辑安全、客户端安全、SDK 安全、隐私合规、安全审计、密码算法、代码安全等 13 类。建议具体使用场景如下：

1. 客户端安全、SDK 安全和隐私合规类 3 类安全要求，建议考虑应用软件的具体业务需求场景是否涉及：产品形态涉及客户端的，建议将客户端安全要求纳入；产品形态涉及 SDK 的，建议将 SDK 安全要求纳入；产品涉及客户信息等隐私合规管理范畴的，建议将隐私合规类要求纳入。

2. 除客户端安全、SDK 安全和隐私合规类以外的其他 10 类安全要求，宜纳入。

本项目安全测评类要求及关注项清单如下：

序号	安全测评类	安全要求	关注项 (验证是否存在相关漏洞)	备注
1	组件安全	应采取有效措施，防范 WEB 服务器常见漏洞，如更新补丁、升级版本、禁用不安全配置等。	常见 web 服务器漏洞包括但不限于：IIS、Nginx、Weblogic、Tomcat、Jboss、Websphere、Axis 等服务器常见漏洞	
		应采取有效措施，防范 WEB 应用组件漏洞，如更新补丁、升级版本、禁用不安全开发框架等。	常见 Web 应用组件漏洞包括但不限于：Shiro、Struts2、Fastjson、ThinkPHP、Spring、Log4j 等框架常见漏洞	
2	服务配置安全	应采取有效手段，防范应用服务未授权访问漏洞，对于可配置身份验证的应用，应进行相关配置，添加身份验证。	常见应用服务未授权访问漏洞包括但不限于：Rsync、Redis、Mongobd、Ldap、Elasticsearch、Memcache、Zookeeper 等未授权访问漏洞	
		应采取有效措施，防范服务器配置漏洞，如 WEB 页面及配置文件中	服务器相关信息泄露漏洞 HTTP 不安全方	服务器相关信息泄露漏洞包括但不限于：备份文件、

		不硬编码内部 IP、物理路径、口令、密钥等敏感信息；不应将管理类的端口或页面暴露在互联网上；关闭服务器目录浏览配置；cookie 中不存储口令等敏感信息；禁用不安全的 HTTP 方法等。	法 Cookie 存储敏感信息	未引用文件、Web 应用敏感信息、目录和管理界面、Cookie 敏感信息
3	会话安全	应采取有效措施，防范会话管理漏洞，如设置 cookie 安全属性等。	不安全的 cookie 属性 会话伪造 会话超时 会话令牌安全性	
4	数据安全	应采取有效措施，保证敏感数据在存储、传输过程中的机密性、完整性，如加密传输、加密存储、异常信息不返回等。	通讯协议安全性 未加密存储数据 敏感信息泄漏	典型的敏感数据包括但不限于鉴别鉴证类信息（如口令、指纹、人脸等）、身份标识信息（姓名、身份证号、手机号、卡号）等
5	通用漏洞防范	应采取有效措施，防范各类应用安全漏洞，如 XSS(跨站脚本)、SQL 注入、命令注入、路径遍历、文件上传等。	XSS 注入类漏洞 文件上传 反序列化漏洞 文件包含 SSRF 重定向	注入类漏洞包括但不限于：SQL 注入、LDAP 注入、XPath 注入、代码注入、命令注入、头注入、空字节注入、XML 注入
6	身份认证	应采取有效措施，防范认证失效的风险，如建立安全的访问控制机制、认证失败回显相同提示信息、设置用户最大连续认证失败次数限制、认证流程校验、采用安全的验证码机制、采用强口令策略、采用安全的传输协议，并对密码进行字段级加密等。	暴力破解 弱口令 通讯协议安全性	
7	业务逻辑安全	应采取有效措施，防范业务逻辑漏洞，如对参	越权类漏洞、 工作流程逃逸漏	

		数进行长度/类型/范围合法性校验、校验用户Session、对下载文件的文件名进行过滤、对业务流程进行验证、重要交易具备防重放措施、通过随机数等方式防范跨站请求伪造等。	洞 请求篡改漏洞 敏感信息泄露漏洞 未授权访问漏洞	
8	客户端安全	应采取有效措施,防范客户端安全风险,如App自身安全风险、程序源文件安全风险、数据存储安全风险、通信数据传输安全风险、身份认证安全风险、内部数据交互安全风险、HTML5安全风险、恶意攻击风险、二进制代码风险、Zipper Down 解压漏洞等。	Janus 签名机制漏洞 应用签名未校验风险 动态调试攻击风险 威胁数据安全问题 密钥硬编码漏洞 zip 文件解压目录遍历漏洞 应用签名未校验风险 动态调试攻击风险 应用数据任意备份风险 界面劫持风险	调试日志函数调用风险 数据库注入漏洞(动态检测) AES/DES 加密方法不安全使用漏洞 RSA 加密算法不安全使用漏洞 密钥硬编码漏洞 动态调试攻击风险(动态检测) Webview 远程调试风险 应用数据任意备份风险 敏感函数调用风险 数据库文件任意读写漏洞 全局可读写的内部文件漏洞 SharedPreferences 数据全局可读写漏洞 SharedUserId 属性设置漏洞 Internal Storage 数据全局可读写漏洞 getDir 数据全局可读写漏洞 FFmpeg 文件读取漏洞 Java 层动态调试风险

				剪切板敏感信息 泄露漏洞 内网测试信息残留漏洞 随机数不安全使用漏洞 代码残留 URL 信息检测
9	SDK 安全	SDK 应参照《银行第三方软件开发工具包（SDK）安全接入指南》（JR/T 0231—2021）要求设计，实现资源控制、身份认证、访问控制、数据安全、软件容错、攻击防护、安全审计相关要求。	Janus 签名机制漏洞 应用签名未校验风险 动态调试攻击风险 威胁数据安全问题 密钥硬编码漏洞 zip 文件解压目录遍历漏洞 应用签名未校验风险 动态调试攻击风险 应用数据任意备份风险 界面劫持风险 数据非法外发 敏感权限未授权使用 自启动或关联启动	
10	隐私合规	应满足个人信息保护要求，如公开收集使用规则、明示收集使用个人信息的目的/方式/范围、征得用户同意后收集使用个人信息、按法律规定提供删除或更正个人信息功能或公布投诉/举报方式等信息、应用分发平台上的 APP 信息应明示到位、管理责任应落实到位，尊重个人信息处理活动中的个人权利；不得收集与提供的	违反必要原则收集个人信息 未明示收集使用个人信息的目的、方式和范围 未经用户同意使用个人信息 强制用户使用定向推送功能 过度索取权限	

		服务无关的个人信息、不得未经同意向他人提供个人信息、APP 不得频繁自启动和关联启动、不得欺骗诱导用户下载 APP、扰乱竞争秩序、侵害用户权益，应避免敏感个人信息处理问题、个人信息跨境提供问题等。		
11	安全审计	应提供覆盖每个用户的安全审计功能，明确应用系统重要安全事件，并记录重要安全事件的审计日志等。	审计日志：未对重要操作和事件记录日志；日志记录不完整（未包含用户 ID、时间、结果等）	
12	密码算法	软件应使用安全性得到广泛认可的算法及协议版本，并遵守安全实现，优先支持国密算法（SM4：密钥长度至少 128bits、SM2：密钥长度至少 256bits、SM3），禁用不安全的算法及协议版本（DES、SHA-1、MD5、RSA1024）。	使用不安全的密码算法	
13	代码安全	外购软件不应包括任何削弱应用安全性的代码，包括：病毒、时间炸弹、后门、木马、复活节彩蛋及所有其它形式的恶意代码。	命令执行类漏洞敏感信息泄露 代码中包含不安全代码	代码中包含不安全代码包括不限于：病毒、时间炸弹、后门、木马、复活节彩蛋及所有其它形式的恶意代码

附件：第三方及开源组件清单、漏洞技术评估和协议合规审查情况说明

说明：第三方及开源组件是指嵌入应用系统并随应用系统部署和运行的软件。

第三方及开源组件清单及漏洞排查结果应包括如下 2 项内容：
1.自评估审查情况说明。
2.本项目使用第三方及开源组件清单。

本项目使用第三方及开源组件漏洞技术评估和协议合规审查情况说明：

（若技术评估、合规审查未发现问题）经排查，未发现本项目使用上述第三方及开源组件存在安全漏洞及协议合规问题。后续如有发现安全漏洞，将及时报告中国农业银行股份有限公司并且配合进行开源组件升级等整改或给出风险缓释措施。

（若技术评估、合规审查发现风险且风险可控）经排查，发现本项目使用上述第三方及开源组件存在安全漏洞及协议合规问题，经过分析，在实际使用场景中，不会产生风险。后续如有发现安全漏洞，将及时报告中国农业银行股份有限公司并且配合进行开源组件升级等整改或给出风险缓释措施。

本项目使用第三方及开源组件，乙方从漏洞技术评估及协议合规审查方面的排查结果如下：

组件集名称	组件名称	组件版本号	组件类型	许可证协议	依赖类型	组件风险等级
例子： <i>commons-io</i>	<i>commons-io</i>	<i>2.5</i>	<i>Maven</i>	<i>Apache 2.0</i>	<i>直接使用</i>	<i>安全</i>
例子： <i>log4j</i>	<i>log4j</i>	<i>1.2.17</i>	<i>Maven</i>	<i>Apache 2.0</i>	<i>间接依赖</i>	<i>严重</i>

--	--	--	--	--	--	--

填写说明：

组件集名称、组件名称、版本号：填写范围包括但不限于 maven、npm、nuget、pip 等常见的包管理工具管理的组件及非包管理的组件。以 maven 组件为例：组件集名称为 groupId、组件名称为 artifactId、版本号为 version；以 npm 组件为例，组件集名称为空；以 python 组件为例。组件集名称为空。

许可证协议：组件中所声明的许可证协议，常见的 maven、npm、pypi 类型组件许可证协议可通过 mvnrepository.com、npmjs.com、pypi.org 网站查询。

依赖类型：表示该组件是被采购项目直接使用还是间接依赖。

组件风险等级：漏洞风险等级参照 CVSS3.0 等级定义，10-9 分为严重漏洞，8.9-7 分是高危漏洞，6.9-4 分是中危漏洞，3.9-0.1 分是低危漏洞。当组件存在一个漏洞时，组件风险等级为该漏洞的风险等级；组件存在多个漏洞时，组件风险等级取所有漏洞风险等级中的最高等级；组件不存在漏洞时，组件风险等级为安全。

漏洞编号列表：当组件存在漏洞时，应列出该组件的全部漏洞编号（多个漏洞时，以逗号分隔），漏洞编号来源自 CVE、CNVD、CNNVD。

漏洞风险评估：当组件存在漏洞时，乙方应参考漏洞编号对应的漏洞详情，分析漏洞影响，并出具相关情况说明。

附件：第三方及开源基础软件清单、漏洞技术评估和协议合规审查情况说明

注：基础软件是指可以独立部署、独立运行，为应用系统提供基础服务的软件，包括操作系统、数据库、中间件等。

- 第三方及开源基础软件清单及漏洞排查结果应包括如下 2 项内容：

 1. 自评估审查情况说明。
 2. 本项目使用第三方及开源基础软件清单。

本项目使用第三方及开源基础软件漏洞技术评估和协议合规审查情况说明：

（若技术评估、合规审查未发现问题）经排查，未发现本项目使用上述第三方及开源基础软件存在安全漏洞及协议合规问题。后续如有发现安全漏洞，将及时报告中国农业银行股份有限公司并且配合进行开源基础软件升级等整改或给出风险缓释措施。

（若技术评估、合规审查发现风险且风险可控）经排查，发现本项目使用上述第三方及开源基础软件存在安全漏洞及协议合规问题，经过分析，在实际使用场景中，不会产生风险。后续如有发现安全漏洞，将及时报告中国农业银行股份有限公司并且配合进行开源基础软件升级等整改或给出风险缓释措施。

本项目使用第三方及开源基础软件，乙方从漏洞技术评估及协议合规审查方面的排查结果如下：

软件名称	软件版本号	许可证协议	依赖类型	软件风险等级	漏洞编号列表	软件风险评估
例子: <i>mysql</i>	<i>8.0.30</i>	<i>LGPL</i>	<i>直接使用</i>	<i>安全</i>		
例子: <i>mysql-driver</i>	<i>1.2.5</i>	<i>apache</i>	<i>间接依赖</i>	<i>中危</i>	<i>CVE-20XX-XXX,</i> <i>CVE-20XX-YYY</i>	<i>逐一针对漏洞编号列表中的漏洞进行分析</i>

填写说明：

软件名称、版本号：基础软件的名称和版本号。

许可证协议：基础软件中所声明的许可证协议，可通过软件官网查看。

依赖类型：表示该基础软件是被采购项目直接使用还是间接依赖。

软件风险等级：漏洞风险等级参照 CVSS3.0 等级定义，10-9 分为严重漏洞，8.9-7 分是高危漏洞，6.9-4 分是中危漏洞，3.9-0.1 分是低危漏洞。当软件存在一个漏洞时，软件风险等级为该漏洞的风险等级；软件存在多个漏洞时，软件风险等级取所有漏洞风险等级中的最高等级；软件不存在漏洞时，软件风险等级为安全。

漏洞编号列表：当基础软件存在漏洞时，应列出该软件的全部漏洞编号（多个漏洞时，以逗号分隔），漏洞编号来源自 CVE、CNVD、CNNVD。

软件风险评估：当基础软件存在漏洞时，乙方应参考漏洞编号对应的漏洞详情，分析漏洞影响，并出具相关情况说明。