**重庆三峡银行**

**零信任安全平台项目**

**询比文件**

|  |  |  |
| --- | --- | --- |
| **采购人** | **重庆三峡银行股份有限公司** | （采购人公章） |
| **发布时间** | **2025年4月** |

目录

[第一章 询比公告 2](#_Toc32729)

[第二章 响应人须知 6](#_Toc9526)

[第三章 项目要求 13](#_Toc27311)

[第四章 评审办法（综合评估法） 34](#_Toc32133)

[第五章 合同模板 39](#_Toc20340)

[第六章 响应文件格式 87](#_Toc24001)

# 第一章 询比公告

为了进一步提升移动办公类远程访问的网络安全，降低网络攻击风险，保障数据和应用系统的访问安全，提供更精细化和多样化的认证方式和访问控制，打造更加安全高效的协同办公体系。现对重庆三峡银行零信任安全平台项目进行公开询比，特邀请有意向的潜在响应人参与响应。

## 1. 询比项目内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 项目名称 | 最高限价 | 成交供应商  数量 | 备注 |
| 1 | 重庆三峡银行零信任安全平台项目 | 230万元 | 1 | 含税 |

## 2. 响应人资格要求

2.1 响应人应当具备承担询比项目的能力

【提供：1、响应人有效营业执照（副本）或事业单位法人证书（副本）或个体工商户营业执照或有效的自然人身份证明或直属的分支机构的总公司的授权委托书；2、响应人法定代表人/分支机构负责人的身份证明；3、授权委托书（如有，适用于有委托代理人的情况时采用）】

2.2 响应人应具有良好的商业信誉和健全的财务会计制度，具有履行合同所必需的设备和专业技术能力，有依法缴纳税收和社会保障金的良好记录，三年内在经营活动中没有重大违法记录【提供书面声明】；

2.3 本项目不允许任何形式的转包【提供书面声明】。

2.4 法人及法定代表人没有被人民法院列为失信被执行人名单【提供：1、法人在中国执行信息公开网的查询截图并加盖单位鲜章；2、法定代表人在中国执行信息公开网的查询截图并加盖单位鲜章】；

2.5 本次询比不接受联合体响应。

2.6 2022年1月1日至2025年1月1日（以合同签订时间为准），具有软件定义边界（SDP）和统一身份认证（IAM）的国产化实施案例均不少于1个，其中软件定义边界（SDP）案例的合同内产品名称或建设内容包含“零信任(SDP)/软件定义边界(SDP)”中任意一个关键内容或字样），统一身份认证（IAM）案例的合同内产品名称或建设内容包含“统一身份认证(IAM)/统一认证(IAM)/身份认证(IAM)/身份管理(IAM)”中任意一个关键内容或字样。低于1个案例（不含1个）取消响应资质【提供：1、合同关键页（合同关键页包含：甲乙双方名称、双方印章、项目名称、合同签订时间、服务范围。）；2、项目简介（格式自拟）；3、合同对应的发票之一（网上税务系统查询（https://inv-veri.chinatax.gov.cn/）该发票的截图，发票开具日期须晚于合同签订日期、发票购买方须与合同买方一致、发票销售方须与合同卖方（响应人）一致）。】

2.7 响应人获得ISO27001（信息安全）资质认证；获得CMMI3级认证。【提供认证证明材料】

2.8 响应人注册成立时间不少于3年，且近3年财务状况稳定【注册成立时间提供营业执照；财务状况提供书面声明】；

2.9 响应人须为产品原厂商，具备对产品二次开发及维护能力【提供书面声明】。

注:以上证明文件若采购人存疑，响应人需提供原件备查，响应文件中须附相关证明文件复印件并逐页加盖公章。

本次询比不接受曾因响应人的违约行为与采购人发生过纠纷的响应人；不接受与采购人合作过程中不遵守询比文件及合同约定的响应人；不接受曾在采购人项目中存在弄虚作假行为的响应人。若响应人存在上述情况，采购人将有权随时取消其响应资格或成交资格（若签署合同后发现的则有权解除合同），没收其响应保证金，并追究其相应的法律责任。截至挂网日，存在上述情况的公司已纳入下列清单。

|  |  |
| --- | --- |
| 序号 | 公司 |
| 1 | 依米康软件技术（深圳）有限责任公司 |

## 3. 询比文件的获取

3.1 响应截止时间：2025年5月15日9时30分（北京时间）

3.2 获取时间和方式：从2025年4月30日到响应截止时间，在重庆市公共资源交易网（www.cqggzy.com）下载询比文件。

3.3 响应人在下载询比文件后，应仔细检查询比文件的所有内容，如有残缺或文字表述不清，以及存在错、碰、漏、缺、概念模糊和有可能出现歧义或理解上的偏差的内容等应在2025年5月3日17时00分（北京时间）前自行在重庆市公共资源交易网（http://www.cqggzy.com/）询比公告的“我要提问”栏目匿名提出。响应人未提出，则视为响应人已全面确认询比文件内容。

3.4 采购人在认为有必要对响应人所提问题进行答复或对询比文件进行补充时，将在《重庆市公共资源交易网（www.cqggzy.com）》“答疑补遗”栏上发布答疑补遗文件。不论响应人下载与否，都视为响应人收到有关本项目在《重庆市公共资源交易网（www.cqggzy.com）》上发布的所有资料并全部知晓有关询比过程和事宜，由此产生的一切后果由响应人自负。

## 4. 响应保证金的递交

4.1 响应保证金的金额： **46,000 元整（大写： 肆万陆仟元整 ）**。

4.2 响应保证金缴纳方式：响应人从响应人的银行账户，通过转账或电汇方式直接划付至对应标段公告下方指定的账户（任选其一），否则，响应保证金无效。响应人自行考虑汇入到账时间风险，本项目响应保证金不接受任何形式保函（包括电子保函）；

**响应人可在付款凭证备注栏中注明项目简称。可简写成：三峡银行零信任安全平台项目。**

4.3 响应保证金递交的截止时间同响应截止时间。响应保证金以重庆市公共资源交易中心询比现场展示的保证金交纳情况为准。

4.4 响应保证金专用账户如下：

详见重庆市公共资源交易网（www.cqggzy.com）对应本项目询比公告信息栏中的保证金信息。

## 5. 市场主体信息登记

根据重庆市公共资源交易中心《关于开展公共资源交易市场主体信息登记工作的公告》的要求，响应人在响应前需在重庆市公共资源交易网（www.cqggzy.com）办理市场主体信息登记手续。若响应人未及时完成市场主体信息登记将不能正常登录电子招投标系统(www.cqggzy.com/EpointSSO/login/oauth2login)查看和办理本项目相关事宜，由此导致无法完成响应的，责任自负。

## 6. 响应文件的递交

6.1 响应文件现场递交时间为2025年5月15日9时00分(北京时间)至响应截止时间。

6.2 递交地点为重庆市渝北区青枫北路6号渝兴广场B10栋重庆市公共资源交易中心开标区（具体请登录重庆市公共资源交易网（www.cqggzy.com）查询或递交文件当日见交易中心大厅电子显示屏）。

6.3 逾期送达的响应文件，不予接收。

## 7. 发布公告的媒介

本次询比公告同时在《重庆市公共资源交易网（www.cqggzy.com）》《重庆三峡银行官网（https://www.ccqtgb.com）》和《中国招标投标公共服务平台（http://www.cebpubservice.com）》上发布。

## 8. 联系方式

|  |  |
| --- | --- |
| 8.1 项目需求咨询 | |
| 项目联系人：张建、周苍 | 联系方式：19936107737、15023212184 |
|  | |
| 8.2 项目流程咨询 | |
| 平台服务机构：重庆联合产权交易所集团股份有限公司 | |
| 平台联系人：罗老师、杜老师 | 联系方式：023-63621694 |
|  | |
| 8.3 采购人联系方式 | |
| 联系人：敬老师 | 联系方式：023-88890395 |
| 采购人地址：重庆市渝北区嘉州路88号中渝国际都会4号写字楼21层 | |

重庆三峡银行股份有限公司

2025年4月30日

# 第二章 响应人须知

## 1. 采购人

重庆三峡银行股份有限公司。

## 2. 响应人

为采购人提供工程、货物和服务的承包商、供货商和服务商。

### 2.1 合格响应人条件

合格响应人应完全符合询比文件第一章中规定的响应人资格条件，并对询比文件作出实质性响应。

### 2.2 响应人的风险

响应人没有按照询比文件要求提供全部资料，或者响应人没有对询比文件在各方面作出实质性响应，可能导致响应被拒绝或评定为无效响应。

## 3. 询比文件

采购人根据自身采购方案或需求编制的采购文件。

询比文件是响应人编制响应文件的依据，是评审委员会评判依据和标准。询比文件也是采购人与成交供应商签订合同的基础。

采购人对询比文件所作的一切有效的书面通知、修改及补充，都是询比文件不可分割的部分。

## 4. 响应

响应人应当按照询比文件的要求编制响应文件，并对询比文件提出的要求和条件作出实质性响应。

### 4.1 响应文件

参与询比活动的响应人按照询比文件的要求编制提交的要约文件的统称。

### 4.2 响应文件组成

响应文件由响应人所作的一切有效补充、修改和承诺等文件组成，响应人应按照第六章“响应文件格式”规定的目录顺序组织编写和装订，否则有可能影响响应人的响应文件评审。

### 4.3 联合响应

本询比项目不接受联合响应

### 4.4 响应有效期

响应有效期为响应截止时间后90天内。

### 4.5 响应保证金

4.5.1 响应人应在响应截止时间前，按询比文件第一章规定向采购人缴纳响应保证金。

4.5.2 响应保证金为响应的有效约束条件。

4.5.3 响应保证金有效期与响应文件有效期一致。

4.5.4 响应保证金币种应与响应报价币种相同。

4.5.5 响应保证金的退还：

采购人在成交通知书发出后2个工作日内将成交通知书和保证金退还通知抄告重庆市公共资源交易中心，重庆市公共资源交易中心在收到保证金退还通知后2个工作日内，向除成交供应商和成交候选人以外的响应人，退还响应保证金。

采购人在合同生效后2个工作日内将签订的合同和保证金退还通知抄告重庆市公共资源交易中心，重庆市公共资源交易中心在收到保证金退还通知后2个工作日内，向成交供应商和成交候选人退还响应保证金。

响应保证金专用账户由重庆市公共资源交易中心制定，关于保证金相关情况的问题请咨询重庆市公共资源交易中心，联系电话023-63621694。

4.5.6 响应人有下列情形之一的，响应保证金将不予退还：

4.5.6.1 响应人在响应有效期内撤销响应文件的；

4.5.6.2 响应人在响应过程中弄虚作假，提供虚假材料的；

4.5.6.3 成交供应商无故弃选或无正当理由不与采购人签订合同的；

4.5.6.4 成交供应商将成交项目转让给他人或者在响应文件中未说明且未经询比单位同意，将成交项目分包给他人的；

4.5.6.5 成交供应商拒绝履行合同义务的；

4.5.6.6 其他严重扰乱询比程序的；

### 4.6 响应文件的份数和签署

4.6.1 响应文件一式三份，其中正本一份，副本一份，电子文件一份（U盘），正本和副本的封面上应清楚地标记“正本”或“副本”的字样，副本可为正本的复印件，当副本和正本不一致时，以纸质正本为准。电子文件应为响应文件盖章后的PDF格式扫描件，文件名为“响应人单位名简称+项目名简称”。

4.6.2 响应文件正本中，每一页均应由响应人加盖公章，其中规定格式的文件应当按要求签名和加盖响应人公章。

4.6.3 若响应人对响应文件的错处作必要修改，则应在修改处加盖响应人公章或由法人或委托代理人签字确认。

4.6.4 电报、电话、邮寄、传真形式的响应文件概不接受。

### 4.7 响应文件的密封与标记

响应文件的正本、副本、电子文件装入一个文件大袋进行密封。密封袋上注明项目名称、响应人名称及“不准提前启封”字样。信封的封口须加盖响应人公章或授权代表签字。

如果未按上述规定进行密封和标记，则其响应将作为无效响应处理。

### 4.8 响应报价

4.8.1 响应人应严格按照“响应文件格式”填写报价。

4.8.2 响应人的报价为一次性报价，即在响应有效期内响应价格固定不变。

4.8.3 本项目只接受一个响应报价，有选择的或有条件的响应将不予接受。

4.8.4 响应报价不得高于最高限价。

### 4.9 修正错误

若响应文件出现计算或表达上的错误，修正错误的原则如下：

4.9.1 响应文件的大写金额和小写金额不一致的，以大写金额为准；

4.9.2 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

4.9.3 单价金额小数点有明显错位的，应以总价为准，并修正单价；

4.9.4 对不同文字文本响应文件的解释发生异议的，以中文文本为准。

4.9.5 含税金额与不含税金额不一致的，以含税金额为准。

评审委员会按上述修正错误的原则及方法调整或修正响应人响应报价，如涉及多次修正，则按上述原则的顺序进行修正。响应人授权代表同意并签字确认后，调整后的响应报价对响应人具有约束作用。如果响应人不接受修正后的报价，则其响应将作为无效响应处理。

## 5. 询比程序

主持人按下列程序进行询比：

5.1 宣布询比纪律；

5.2 宣布采购人、唱标人、记录人、监督人等有关人员姓名；

5.3 公布在响应截止时间前递交响应文件的响应人名称，并点名确认响应人是否派人到场；

5.4 展示响应保证金，响应保证金缴款不全或有误的，则记录在案交由评审委员会评审；

5.5 封装情况检查：响应人或者其推选的代表检查各响应文件的封装情况并确认；

5.6 设有最高限价的，公布最高限价；

5.7 开启响应文件；

5.8 采购人代表、响应人代表、监督人、记录人等有关人员在询比记录上签字确认；

5.9 询比结束。

## 6. 评审

见第四章内容。

## 7. 确定成交供应商

7.1 确定成交供应商原则

采购人按照评审报告中推荐的成交候选人排名顺序确定成交供应商，如成交供应商因不可抗力或者自身原因不能履行合同的，采购人可以重新采购或确定依次其后的候选人为成交供应商，以此类推。

7.2 不承诺最低价格成交。

7.3 若成交供应商响应材料出现造假、不实等与实际查询结果不符或无故弃选的情况，采购人有权选择重新询比或顺延下一成交候选人，由此带来的损失采购人有权通过没收响应保证金等方式进行追溯。

## 8. 签订合同

8.1 采购人指定的使用单位将在自成交通知发出之日起，依据询比文件和成交供应商响应文件的约定，按照采购人内部流程与成交供应商签订书面合同。所签订的合同不得对询比文件和成交供应商响应文件作实质性修改。

8.2 成交供应商在领取成交通知书后，应根据第一章中“联系方式”内容，及时与项目联系人对接，并按采购人要求在规定时间完成合同的签订。如未在规定时间内签订合同，且经采购人书面通知后仍不按照通知要求签订合同的，可视为成交供应商无故弃选。

8.3 询比文件、成交供应商的响应文件及澄清文件等，均为签订合同的依据。

8.4 合同生效条款由供需双方约定，法律、行政法规规定应当办理批准、登记等手续后生效的合同，依照其规定。

8.5 签订合同前后，若成交供应商无法按要求履约或成交单位提供的产品测试不合格或与响应文件中的产品不一致，采购人可以废除成交供应商资格，并可选择按照成交候选人顺位与下一候选人签订合同。

8.6 该项目不允许任何形式的转包。

## 9. 纪律与要求

响应人不得相互串通响应或者与采购人串通响应，不得向采购人行贿谋取成交，不得以他人名义响应或者以其他方式弄虚作假骗取成交；响应人不得以任何方式干扰、影响评审工作。

9.1 有下列情形之一的，属于响应人相互串通响应：

9.1.1 响应人之间协商响应报价等响应文件的实质性内容；

9.1.2 响应人之间约定成交供应商；

9.1.3 响应人之间约定部分响应人放弃响应或者成交；

9.1.4 属于同一集团、协会、商会等组织成员的响应人按照该组织要求协同响应；

9.1.5 响应人之间为谋取成交或者排斥特定响应人而采取的其他联合行动。

9.2 有下列情形之一的，视为响应人相互串通响应：

9.2.1 不同响应人的响应文件由同一单位或者个人编制；

9.2.2 不同响应人委托同一单位或者个人办理响应事宜；

9.2.3 不同响应人的响应文件载明的项目管理成员为同一人；

9.2.4 不同响应人的响应文件相互混装；

9.2.5 不同响应人的响应保证金从同一单位或者个人的账户转出。

9.3 使用通过受让或者租借等方式获取的资格、资质证书响应的，属于以他人名义响应。

9.4 响应人有下列情形之一的，属于弄虚作假的行为：

9.4.1 使用伪造、变造的许可证件；

9.4.2 提供虚假的财务状况或者虚假业绩；

9.4.3 提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；

9.4.4 提供虚假的信用状况；

9.4.5 其它弄虚作假的行为。

针对以上情况，采购人有权没收响应人的响应保证金，并保留进一步追究由此带来损失的权利。

## 10. 提问、质疑、投诉

10.1 补遗内容可能影响响应文件编制的，须在响应截止时间3日前发布，发布时间至响应截止时间不足3日的，须相应延后响应截止时间。

10.2 响应人对询比文件和答疑补遗有质疑的，应当在响应截止时间3日前，以书面形式通知采购人。采购人认为有必要对响应人所提问题进行答复或对询比文件进行补充时，将答复内容以补遗的形式发布。

10.3 响应人对公示的成交结果有质疑，响应人需在公示期内以书面形式向采购人提出质疑。采购人认为有必要对响应人所提质疑进行答复时，将以书面形式进行答复。

10.4 响应人对采购人的答复不满意或者有质疑，可向采购人纪检监察部投诉。

采购质疑邮箱：sx.jcb@ccqtgb.com

采购投诉邮箱：sxyhjjz@ccqtgb.com

## 11. 无效响应条款

响应人或其响应文件出现下列情况之一者，应为无效响应：

11.1 响应人未按询比文件规定在响应保证金递交截止时间内提交足额响应保证金的。

11.2 响应人未通过资格评审、形式评审、响应性评审或响应文件经证实存在弄虚作假的。

11.3 响应人超出其营业执照或事业单位法人证书上经营范围（业务范围）响应的。

11.4 单位负责人为同一人或者存在直接控股、管理关系的不同响应人，不得参加同一合同项下的采购活动。

11.5 同一分包的软件，制造商参与响应，再委托代理商参与响应的。

11.6 响应文件不满足询比文件第六章响应文件格式中所规定签字、盖章的。

11.7 响应文件出现多个响应方案或响应报价的。

11.8 响应报价超出最高限价的。

11.9 响应文件含有违反国家法律、法规的内容，或附有采购人不能接受的条件的。

11.10 出现影响询比公正的违法、违规行为的。

11.11 与采购人、评审专家、其他响应人恶意串通。

11.12 参与响应的法人发生合并、分立、破产等重大变化后，不再具备询比要求的资格条件的。

11.13 提供虚假材料谋取成交资格的。

11.14 响应文件含有采购人不能接受的附件条件的。

## 12. 询比失败情形

12.1 出现以下情形本次询比失败：

12.1.1 首次询比的项目，截至响应截止时间，响应人少于3个的。

12.1.2 经评审委员会评审后否决所有响应的。

12.1.3 法律法规规定的其他情形。

12.2 重新询比和不再询比

重新询比（如第二次询比）的响应人仍然少于三个的，按照有关规定的程序开标和评审。重新询比经评审有有效响应人的，应当确定成交候选人；无有效响应人的，可以不再进行询比。

## 13. 终止询比

13.1 因情况发生变化或其他原因造成该项目取消的，本次询比自动终止，双方互不承担责任，采购人有息退还响应保证金。

13.2 签订合同之前，采购人发现成交候选人经营、财务状况发生较大变化或存在违法行为，采购人认为可能影响其履约能力的，采购人可废除成交供应商或成交候选人资格。

## 14. 参与项目费用

响应人参与本询比项目时，一切与响应有关的费用均由响应人自理。

本项目平台服务费为 15000 元，由成交供应商向重庆联合产权交易所集团股份有限公司支付。成交供应商应在领取成交通知书时一次性缴纳，请各响应人综合考虑进行报价。

# 第三章 项目要求

## **1.** 业务需求

### 1.1 需求概述

基于零信任理念的新一代安全办公体系建设，通过零信任SDP（SDP：Software Defined Perimeter）、统一身份认证（IAM：Identity and Access Management）和即时通讯（IM：Instant Messaging）等模块，构建全新的安全办公体系解决方案，以提升安全防护能力，满足合规要求，并优化用户体验。

（1）构建动态灵活的零信任SDP。零信任SDP根据用户信息、设备状态、地理位置、时间窗口、设备特征（如要求安装并开启了指定的杀毒软件才能接入）、用户行为等因素，实现了多维度的精细化管理，使访问策略可以精准细化到每个独立个体，最小化潜在的风险面。每个请求都经过严格的验证和授权过程。对外部隐藏内部网络结构和敏感服务，只有通过SPA（Single Packet Authorization）单包认证后才能建立连接，减少攻击面，而不是传统基于网络边界的控制列表ACL（Access Control List）,提升资源访问的安全性，增强策略的灵活性，更好地适配多样化的业务需求。

零信任SDP模块提供了一个安全的接入环境，利用基于身份的访问控制和权限认证机制，让内部应用和服务“隐身”。当黑客试图进行攻击时，会发现看不到目标而无法攻击，只有获得权限的业务人员可以正常访问，确保内部资源不受外部威胁，同时通过持续的身份验证和设备检查实现主动防御能力。降低潜在的安全风险，增强整体的安全性。

（2）建设统一身份认证IAM。为人员身份、认证、授权的全场景提供基础服务，涵盖身份管理、统一认证、多因素认证（MFA）、认证风险控制、权限控制及身份管理与认证审计。通过这些功能，IAM集中管理和维护所有用户的身份信息，确保数据的一致性和准确性，形成用户统一身份信息，实现从入职到离职的全生命周期管理。

作为零信任安全架构的核心，IAM以身份ID为中心构建身份认证管理系统，将用户身份作为重要的安全防护要素。系统默认对用户身份“不信任”，持续认证用户身份，并根据实时行为动态调整访问权限。IAM通过持续检测用户行为风险，提供多系统间的单点登录（SSO）体验，又保障访问的高安全性。

（3）打造零信任防护的即时通讯IM。在零信任建设中，构建一个以IM为入口的办公APP，覆盖消息、协同办公、任务管理、互联互通等多层面功能的一站式平台。该平台将内部系统与应用整合为卡片式设计，融入即时通讯工作台，成为员工的统一办公入口。

通过集成零信任SDP SDK，减少终端侧APP的数量，提供了安全沙箱能力和细粒度的数据安全控制（如应用只能在APP内打开、只能在线查看、防截屏、敏感信息脱敏展示等能力），从而简化操作流程，提高协同效率，使员工只需通过即时通讯界面即可便捷访问所有应用与服务，构建一个高效、安全且易用的办公工作台。

**本项目通过复用现有的OA系统自带的即时通讯E-Mobile软件进行优化集成**。通过对现有即时通讯E-Mobile软件性能优化和安全升级，作为员工便捷访问所有应用与服务的统一入口，提升整体办公平台的效率，满足企业对数据安全、统一管理和用户体验的高标准要求。

### 1.2 功能要点

主要功能如下表所示：

|  |  |  |
| --- | --- | --- |
| 零信任SDP | 控制中心 | 控制中心部署在企业的内部私有服务器上，通过管理平台，管理员可以管理和查看，主要功能包括：零信任办公策略管理、全网终端资产管理，安全策略管理，管控策略管理，安全准入管理、数据防泄漏管理、日志审计管理等。 |
| 零信任接入网关 | 部署在互联网及内网可达区域，以便互联网终端、内网终端均可无障碍访问无边界接入网关，从而顺利访问企业后端业务系统。控制中心及无边界网关，均可支持高可用部署架构，并可根据实际业务访问量及并发负载，进行水平扩展，保证访问企业后端业务系统的连续可用性。 |
| 终端零信任接入 | 在终端上为用户提供零信任接入入口 |
| 终端管控 | 提供终端管控等功能，支持Win、Mac、Linux、Android、IOS、鸿蒙操作系统终端安全检测能力。 |
| 水印保护 | 支持对终端设置屏幕及打印明、暗水印，对于截屏、拍照等泄露方式可追溯查找泄露源 |
| 统一认证平台（IAM） | 统一身份 | 机构管理、角色管理、凭证管理、自助服务等 |
| 统一认证 | 提供通用目录服务、域认证、应用SSO、认证管理、会话管理、多因素认证（MFA）等 |
| 统一权限 | 权限建模、平台权限、权限合规等 |
| 监控预警 | 访问时间、地点、设备、黑白名单、风险策略等 |
| 合规审计 | 账号审计、登录审计、操作审计、访问审计、认证审计等 |
| 移动办公安全防护 | 数据安全 | 实现APP内隔离的安全工作空间、安全水印、防截屏、打印管控等功能，实现存储、网络、应用、外设等隔离，形成端、网、业务、文件、数据的全周期访问控制闭环，解决数据落地泄漏问题，保障数据全生命周期安全。 |
| 工作台安全 | 为工作台的单点登录应用系统提供统一的零信任安全防护，实现单点登录系统零改造。 |

### 1.3 核心要点详细信息

|  |  |
| --- | --- |
| 功能分类 | 详细描述 |
| 身份管理 | 1. 组织管理：支持定义多套组织维度，自定义组织属性（如名称、编码、描述等），以树形结构展示组织，可扩展组织属性。具备组织查询、新增、删除、修改、迁移、合并、排序功能，能设置组织岗位范围和默认岗位，支持组织导入导出。 |
| 2. 组织模型管理：支持定义多套组织维度，每个维度下可自定义组织属性（唯一性、必填性、可见性、显示顺序等），通过正则表达式与字典约束属性内容，可灵活调整组织机构及所属人员。 |
| 3. 用户管理：支持自定义用户类型（内部用户、外部用户、临时用户等），每个用户类型可自定义用户属性（如姓名、性别、联系方式等）。以树形组织用户结构呈现，支持用户查询、新增、删除、修改、迁移、排序、设置主副部门、设置岗位、导入、导出操作。 |
| 4. 用户模型管理：支持自定义多种用户类型，每个用户类型可对用户属性进行详细设置（是否唯一、必填、管理员是否可见、用户是否可自助编辑、显示顺序等），支持正则表达式与字典约束属性内容，以及属性脱敏配置（如手机号、身份证号脱敏）。 |
| 5. 用户组管理：支持用户组新增、删除、修改、查看。可按部门、人员及规则添加用户到用户组，规则包括定义多个分组策略（分组策略内条件为与关系，分组策略间为或关系），支持按部门范围、部门属性（等于、不等于等多种匹配规则）、用户属性（等于、不等于等多种匹配规则）定义分组策略，支持添加人员到用户组，支持用户自动分组策略排除用户管理（排除用户不受自动分组策略影响，可查看、修改）。 |
| 6. 数据源同步：支持通过 LDAP 拉取、DB 拉取、FTP 拉取、API 拉取、API 推送、Excel 初始化等方式，从企业微信、钉钉、飞书等办公平台通过标准接口同步数据，整合企业零散的组织用户数据，形成权威的组织用户体系，根据不同应用所面向的用户进行按需同步。 |
| 7. 数据源同步流程装配：支持配置身份数据同步过程中的处理事件动作，涵盖从上游身份源到 IAM 平台数据，再到下游应用的整个流程，流程分为数据预处理（数据传入 IAM 平台，落入数据库前的处理动作，如数据预调整）、事件动作（数据落入数据库未提交时的处理动作，同步任务，失败则数据回滚）、任务动作（数据成功落入数据库提交后的处理任务，异步任务，按 IAM 平台调度执行）三个模块。 |
| 8. 身份集成配置：支持把平台组织、用户、岗位、自定义对象等数据同步给下游应用系统，支持定义多个应用系统数据同步策略，可通过 API 拉取、API 推送、LDAP 推送、FTP 推送等方式进行配置。 |
| 9. 用户密码策略：支持用户默认密码策略、用户随机密码 + 通知策略。可配置是否启用强制修改初始化密码策略、密码有效期策略（设置密码有效期、过期提醒时间、过期强制修改时间、提醒方式）、历史密码检测策略（用户不能使用最近三次历史密码作为新密码）、弱密码检测策略（开启时对用户修改密码等场景检测，支持弱密码库管理与规则定义）、自定义密码复杂度策略（以及根据用户、用户组设置）、密码策略白名单管理（加入白名单用户不受多种密码策略限制）、AD 密码反向同步策略（保证 AD 与 IAM 用户密码一致性），可按用户类型、指定用户、组织机构、自定义范围（用户属性）条件分别进行密码策略配置。 |
| 10. 用户数据同步：具备业务侧与网络侧的用户数据同步能力，在统一身份认证功能中创建或删除组织和用户后，零信任功能中相应数据应同步创建或删除，实现统一的组织和账号管理。 |
| 应用管理 | 1. 应用信息管理：支持管理接入系统的各类应用（BS 端应用、CS 端应用等）基础信息。应用管理界面支持按应用名称、应用分类、应用形态、应用认证协议筛选应用，应用列表显示应用名称、图标、形态、认证协议、分类、状态、创建时间、修改时间，支持应用的创建、编辑、删除、查看详情操作。 |
| 2. 应用授权管理：支持接入系统导入授权，以及按照用户组、用户进行授权。应用授权界面可查看应用授权详情（用户姓名、账号、授权来源），支持导入应用授权、授权应用给用户和用户组。 |
| 3. 应用账号管理：支持应用自定义账号策略和身份即账号策略，允许管理员对应用组织与账号进行管理，提供应用账号自动生成策略、存量应用账号自动绑定用户策略、用户通过门户绑定自助绑定应用账号策略。实现灵活的应用账号管理，包括分配、锁定、回收、停用等管理，一人多账号场景管理，孤儿账号管理，公共账号管理，支持设置长期未使用的账号为闲置账号（可自定义闲置账号时长，支持自动或手工禁用闲置账号）。 |
| 4. 应用数据同步：具备业务侧与网络侧的应用数据同步能力，在统一身份认证功能中创建或删除应用后，零信任管理平台中相应应用应同步创建或删除，实现统一应用管理。 |
| 认证管理 | 1. 认证协议管理：支持多种认证协议，BS 端系统单点登录支持 Cas、Oauth、OIDC、SAML、JWT、RADIUS、RESTFUL、PORTAL 等协议及密码代填，提供 SDK 供应用系统快速集成；CS 端系统单点登录支持 Oauth 协议与密码代填；移动端免密认证支持 Android、iOS、H5 移动应用形态，支持 Scheme 唤起、集成 SDK 唤起、APP 微门户；支持 Radius、LDAP、tacacs + 认证协议，支持 802.1X 以及 portal 认证协议。 |
| 2. 认证源管理：支持多种认证方式（密码认证、扫码认证、动态口令认证、短信认证、邮箱认证、消息认证、推送认证、临时授权、人脸认证、CA 认证、AD 域认证、第三方认证等），每种认证方式可配置不同的认证源。支持创建多个外部 AD/LDAP 认证源、外部 API 密码认证源，数据源同步时指定用户密码认证源，管理员可切换用户密码认证源；扫码认证支持认证 APP 扫码、多个企业微信 APP 扫码等多种 APP 扫码及多码合一技术；动态口令认证支持认证 APP 在线令牌、企业微信小程序令牌等多种令牌；消息认证支持通过企业微信、钉钉、飞书消息通道发送验证码进行认证，支持设置多个消息通道，实现消息通道合一，平台智能识别用户消息通道；第三方认证支持创建企业微信、钉钉、飞书认证源用于单点登录，支持创建基于标准认证协议的第三方 IDP（标准认证协议支持 Cas、Oauth、OIDC、SAML、JWT）。 |
| 3. 认证策略管理：支持登录策略和访问策略。登录策略可按应用、网络、时间、用户行为因子设置访问控制策略（如配置会话有效时间、登录失败锁定次数、登录页有效期、密码到期提醒、控制策略优先级、用户禁用状态监测、用户锁定状态监测等全局策略）；访问策略可按用户、用户组、应用、应用账号、网络、时间、用户行为因子设置访问控制策略，访问控制策略支持提升认证（执行认证级别、执行认证方式）、拒绝登录。 |
| 4. 认证设备管理：支持对移动认证设备和 PC 设备进行管理，可查看设备信息（用户账号、设备名称、操作系统版本、设备指纹、设备风险、设备状态信息），支持对设备进行删除、锁定、解锁操作。 |
| 5. 单点登录联动：具备业务侧与网络侧的单点登录联动能力，实现应用门户单点和业务应用单点登录。通过零信任客户端，在统一身份认证功能中创建应用并授权给用户，在零信任功能中创建统一门户应用并授权给用户，用户登录零信任客户端后可直接单点访问授权应用。 |
| 权限管理 | 1. 多种权限模型：支持 RBAC、ACL、DRBAC、ABAC 等多种权限模型，可根据应用系统情况选择配置，设置具体参数（如角色、权限对象等），提供属性定义（权限对象、数据字典等编辑与添加操作），可设置权限授权有效期与权限申请有效期。 |
| 2. 应用权限体检：支持权限检查功能，能够展示系统中未授权账号、违反互斥账号、敏感权限账号、相似角色、静默角色、静默功能权限、静默数据权限，选中其中一项能够跳转查看具体账号权限情况。 |
| 3. 权限合规检测：支持权限合规检查与敏感权限管理能力，可设置合规规则、互斥规则（系统互斥、角色互斥、菜单互斥以及行为互斥）、业务角色互斥（业务角色互斥与业务系统角色互斥），进行规则扫描，查看用户合规审计与应用合规审计，提供敏感权限管理（包括角色、菜单权限、按钮以及数据权限）。 |
| SDP - IAM 联动 | 零信任平台与统一认证平台（IAM）无缝对接，从 IAM 同步账密、机构、应用等数据及状态信息（如禁用状态、绑定状态），自动同步 IAM 用户与应用的授权关系，在应用门户展示用户可访问的应用（与 IAM 中相同用户权限一致），简化运维流程。 |
| 终端管理 | 1. 终端分类管理：支持提供设备动态分类以及设备管理的能力，可添加设备分类策略（如企业设备分类策略：【终端在域中】AND【终端运行任意一款杀毒软件】；僵尸设备分类策略：设备超过 1 天不活跃；未命中以上分类策略的设备均为 BYOD 设备）。可查看不同分类设备信息，对设备执行强制注销操作，不同分类设备登录客户端后展示不同信息。 |
| 2. 终端设备激活：支持提供灵活判断终端设备绑定方式的功能（一对一、一对多绑定等），为注册成功终端设备颁发可信设备身份。可创建多种设备绑定策略（如企业设备自助绑定策略、企业设备人工审批策略、BYOD 设备人工审批策略、BYOD 设备禁止绑定策略），根据不同条件（终端是否在域中、是否运行杀毒软件、客户端 IP 等）设置绑定方式（自主绑定、人工审批、禁止绑定），在绑定登录过程中，客户端有相应提示，管理员有审批通知并可进行审批。 |
| 3. 终端准入策略：支持提供持续检测终端环境及终端合规、准入控制的能力。通过零信任客户端采集不同操作系统 PC 环境（高危端口、运行的软件、零信任客户端版本、运行的杀毒软件等）和移动端环境（操作系统版本、零信任客户端版本、系统是否被 ROOT / 越狱等）信息，对 PC 端访问应用进行可信标记，基于终端安全状况和访问进程进行访问控制（如设置系统版本基线策略、合规进程基线策略、风险策略等，根据策略进行安全警告、禁止登录、二次认证等操作）。 |
| 4. 终端限流访问：支持对接入服务进行流量并发保护，下发终端限流策略（如新建限流策略，包括直接转发限速、隧道传输限速，超过速率客户端执行丢弃策略），配置 SDP 服务限流策略后，对终端访问流量进行限速控制，用户访问应用时若流量受限有相应提示。 |
| 5. 智能连接：零信任客户端身份认证登录后支持身份驻留，提升用户访问体验性。平台支持根据身份区分不同接入点 / 接入服务，具备多网关按需接入能力（如设置多个接入点，分别负责不同人群接入，行内、外包人员登录后根据身份自动选择接入点）。 |
| 访问控制 | 1. 应用 ACL 控制：支持仅允许 IP 白名单内的主体访问指定的应用及资源，到期自动回收访问权限。支持基于环境属性（域、位置、时间、IP、信任等级）、客体属性（应用、应用菜单、应用安全标签、菜单安全标签）、操作属性（按钮）等信息的访问控制（如配置允许访问应用资源的 IP 白名单，选择资源认证级别和授权组，对不同用户进行应用和资源授权，用户登录后根据授权访问应用和资源，管理端可查看资源文件下载、浏览信息）。 |
| 2. 动态访问控制：支持提供应用 / 应用资源的动态访问控制能力，支持灵活组合规则得到不同的风险级别（如定义共有设备访问、非可信 IP 访问等规则及风险分值），执行相应的风险处置方式（高风险退出登录、中高风险禁止访问、中低风险短信增强认证、低风险安全示警），可查看风险触发的日志信息（请求时间、用户账号、应用资源、策略名称、风险分值、处置方式、风险明细）。 |
| 3. 应用可信渠道访问：支持针对 http、https 访问协议的应用进行深度报文解析，通过可信浏览器、IM、终端沙箱等渠道进行选择访问（如应用发布时设置可信访问方式，用户通过不同方式访问应用有不同结果）。支持同一应用发布到不同接入点 / 接入服务（如内网网关 / 外网关），满足不同业务场景的安全访问要求（如外网访问应用添加水印，内网访问不添加，用户在内网和外网访问应用时页面显示不同且网关节点不同）。 |
| 4. TCP/UDP 访问控制：支持 TCP、UDP 协议的应用接入（如配置 CS 应用添加 TCP 协议应用，用户通过 Xshell 访问；配置 CS 应用添加 UDP 协议应用，用户设置代理后使用腾讯会议正常通讯）。 |
| 5. 应用资源管理：支持应用概览统计能力（包括应用总数、WEB 应用数、隧道应用数等信息），提升管理员的运维能力。支持 WEB 应用 (7 层）、隧道应用 (3、4 层 TCP/UDP 应用) 的代理和发布，支持虚拟服务发布（实现应用只提供安全访问通道，而不做控制的场景）。支持 WEB 应用数据传递（可通过 URL、Header、Cookie 自定参数传递，满足应用对特定参数的需要，实现对现网应用无需修改即可正常访问），支持 WEB 应用访问透传控制（按照规则对特定 URL 不进行权限检查放过，满足对一些公共可访问的特定 URL 进行例外放行的需要）。 |
| 网络安全 | 1. 网络隐身：支持提供隐藏自身服务端口的能力，未登录和登录零信任客户端时，使用端口扫描工具扫描零信任服务 IP 及 TCP、UDP 端口，服务端均未获取到报文信息，端口扫描工具未扫描到零信任服务端开放任何端口。 |
| 2. 隧道加密：支持提供隧道内传输数据加密，加密方式支持国密算法，具备隧道断线重连的能力。登录零信任客户端访问测试应用时，抓取隧道流量显示为密文，断开网络后重新连接，客户端有隧道重连提示。 |
| 3. 网络隔离：支持提供内外网隔离的能力，开启内外区域隔离策略后，登录零信任客户端无法访问互联网地址，关闭该策略后可正常访问。 |
| 安全防护 | 1. HTTP 转 HTTPS 协议：支持 HTTP 转 HTTPS 协议的应用接入（如添加 HTTP 协议应用域名证书，配置接入应用的访问协议为 HTTPS 并关联证书，用户通过 HTTPS 访问应用可正常登录系统）。 |
| 2. 熔断流量安全保护：执行安全防护策略，保障流量安全。可新增熔断安全防护策略（设置触发保护时间、触发条件、最小请求数、超时时间、失败率阈值等），应用发布时开启熔断防护并选择相应策略，当用户访问应用满足触发条件时，跳转熔断保护页面并记录安全防护日志，熔断保护解除后可成功访问应用。 |
| 3. 风险 IP 封禁保护：智能化 IP 封禁，基于攻击防御信息自动将风险 IP 进行自动阻断。设置封禁策略（统计时间窗、累计防护次数、统计类别、封禁策略、封禁时间、是否禁止境外 IP 访问等），应用配置相应防护策略（如应用 A 配置 WAF 策略、应用 B 配置 CC 防护策略），当用户访问触发相关防护策略时，该用户网络 IP 被封禁，封禁期间无法访问任何受保护应用，封禁时间结束后才可访问。 |
| 4. Session 安全保护：防止攻击者盗用凭证登录系统。将目标应用接入零信任后，用户正常登录提取 Session，攻击者使用该 Session 在其它电脑上访问目标应用时，返回零信任平台阻断页面，可查看到攻击 IP、相应的漏洞 Payload 等阻断日志信息。 |
| 5. 网关 Bypass 功能：当网关遇到问题时，通过 bypass 功能优先保证业务正常运行。启用应用 bypass 功能后，访问应用不再会经过网关的拦截，直接跳转到应用本身页面。 |
| 安全合规审计 | 1. 统计报表：支持提供统计报表能力，通过管理平台查看统计大盘，数据至少包括用户总数、启用用户数、禁用用户数、当前在线用户数等用户信息；终端总数、启用终端数、禁用终端数等终端信息；应用总数、WEB 应用数、隧道应用数、访问应用分布等应用信息。 |
| 2. 日志审计：支持提供日志审计及日志推送能力，可查看用户登录日志、应用访问日志、管理员日志等（包括时间、用户名、登录 IP、操作信息等）。支持配置 syslog 日志推送，可自定义配置发送告警日志或系统日志等，支持发送到多个 syslog 地址，syslog 支持 tcp 和 udp 两种格式。 |
| 数据安全 | 1. 截屏 / 录屏安全防护：对受保护的应用开启 “截屏 / 录屏” 保护策略，支持截屏 / 录屏文件上传审计、截屏 / 录屏文件加密保护、截屏 / 录屏操作告警策略、禁止对此应用截屏或录屏策略（如开启策略后，截屏 / 录屏文件自动上传至服务端，本地无法打开，操作时有告警提示，禁止截屏 / 录屏时有安全提示）。 |
| 2. 数据隔离保护：支持提供数据隔离、应用管控、禁止复制、禁止粘贴、禁止截屏、禁止打印等能力。可指定应用打开渠道，设置复制粘贴保护策略；对内部分发的应用开启 “应用文件隔离”“ |

## **2.** 技术要求

### 2.1 总体原则

系统的建设应遵循集成性、先进性、可扩展性、稳定性、安全性、经济性、前瞻性和可维护性相结合的原则。

2.1.1 集成性：系统建设需充分考虑与其它系统的集成，能快速与采购人其它业务和管理系统的集成。

2.1.2 先进性：软件系统的选择与开发应在满足业务需求的基础上具有易改造、易升级、易操作、易维护等特点。

2.1.3 可扩展性：支持业务和系统的可扩展，支持行业应用可扩展，具有向后兼容的能力。

2.1.4 稳定性：系统要确保系统平稳运行，支持7×24小时连续运行，满足高峰处理的需要。

2.1.5 安全性：

1）系统必须建立在成熟稳定的硬件环境和应用软件基础上，通过完善的备份恢复策略、安全控制机制、可靠的运行管理监控和故障处理手段来保障系统的运行稳定、安全。

2）制定并发布完善的隐私政策，引导客户“主动”阅读知晓；仅保留与业务处理相关的、必须的客户敏感信息，且采取强加密措施进行保存；不应在日志中记录客户支付敏感信息；不允许保留非本机构的客户敏感信息；采用信息输入安全防护、即时数据加密等安全措施防止数据被非法截获。

2.1.6 经济性：系统的建设要考虑在网络、设备、信息安全等方面合理利用现有的资源。要充分调研，结合业务需求，合理利用现有资源，降低系统的投资，创造最优的工作效率，产生最好的经济效益。

2.1.7 前瞻性：系统体系架构和软件体系结构要有前瞻性，要充分考虑未来业务的发展和管理的变化，方便对新业务和新需求的扩展和支持，合理设计系统的规模，使之不仅能满足目前应用的需要，而且能适应将来的发展。

2.1.8 可维护性：系统可维护，运行成本可控。

### 2.2 用户体验要求

界面可根据用户需求灵活更改（增强标签分类特性），注重用户体验，使系统各项功能易见、易学、易用。

客户端界面一致性，支持不同终端适配界面（解决不同终端，屏幕尺寸的视觉差异）。图形显示直观，业务流程支持形象化。遵循20/80原则，配置常用清单、快捷功能，即方便用户快速入手，又大大提升了使用效率。遵循人机交互原则，对用户的错误输入尽早发现并给出提示，对复杂的功能操作，提供操作向导；人性化设计，易操作，遵循用户习惯，让用户有更好的操作体验。支持跨平台、终端适配（支持各类分辨率、各主流版本的浏览器访问）。

### 2.3 系统技术架构要求

1）设计思想、系统架构应兼顾成熟与先进性，系统的搭建与实施原则上应采用目前主流的分布式、微服务架构技术，微服务模块可根据系统性能需要进行灵活的扩展部署，同时确保整体架构在产品生命周期内相对稳定与适用。

2）系统技术架构合理，数据结构合理，避免数据冗余，具有良好的扩展性、维护性和稳定性。如服务限流机制、服务降级机制等服务管控机制的应用，保障系统稳定运行。

3）系统所采用的软件平台具备开放性、通用性、扩展性和安全性。在性能指标达到预警值时，能够通过横向扩展集群模式达到性能的线性增长。系统应具有线性或近似线性的性能扩展能力，并能在不停止服务的的情况下完成容量伸缩。

4）支持自启动服务集群、Kubernetes（K8S）等多样化部署方式，适应云原生发展的需要。应用系统之间逻辑独立、启停服务时系统间不相互影响的部署方案。应用系统还应支持双活跨数据中心的部署方案。

5）系统支持域名部署。

### 2.4 系统性能要求

1）应具有高效的运行效率，能通过负载均衡、流量控制、消息缓存等机制，提供大规模、高并发量的交易处理能力，满足登陆、查询、日终批量等性能需求；

2）系统必须提供平台级的负载均衡和容错能力；

3）主机系统能够保持7\*24稳定的不间断运行，从系统软硬件平台及网络等方面来保证系统的稳定性；

4）可用率：系统总体平均可用率在99.99%以上。

### 2.5 安全性要求

为确保信息安全，采取的措施包括但不限于以下：

1）平台安全：架构设计符合安全性要求，平台软件达到安全设计标准且不低于同业相关系统要求。

2）数据安全：支持文档安全软件整合技术，从而做到数据传输加密、远程安全访问、数据存储加密，数据部署网络区域应支持入侵检测与防御系统、防火墙的应用。

3）容灾备份：支持各种容灾的软硬件设备的使用等。

4）管理安全：提供完善的日志功能，能够记录系统使用人员的关键操作，保证系统应用的安全。

5）密码策略：初始密码强制更改、启用验证码、密码过期控制、密码错误次数控制、密码强度设置等，不得以明文的方式保存任何相关密码，防止暴力破解和恶意攻击。

6）系统严密、灵活的访问安全控制；

7）系统有整体的用户/权限管理体系，可统一进行用户/权限的管理，实现到字段级的查询、修改、管理权限控制；

8）系统开发必须满足采购人软件研发项目安全需求基线要求。

|  |  |  |
| --- | --- | --- |
| 类别 | 子类 | 安全需求 |
| 身份认证 | 口令安全  策略 | 应用系统应具有口令复杂度限制功能，并在设置密码、修改密码、重置密码的时候进行密码复杂度校验：（1）口令复杂度要求：长度8位及以上，至少包含大写，小写字母，数字，特殊字符中的三种或三种以上；（2）不能使用和用户名相同的密码；（3）避免使用默认口令，如果使用，应在用户首次登录时，强制用户修改密码。（4）系统各用户应根据使用场景定期更改密码，可动态设置密码更新周期频率（最长不超过90天）。  （5）密码历史检查机制：用户每次修改密码时，新密码不得与最近几次的密码相同。此“最近几次”的具体次数可由管理员根据安全策略进行配置。 |
| 口令加密  传输 | 用户口令在传输过程中需进行加密，建议使用md5加盐(随机数)、sha2、pbkdf2等方式进行加密传输，禁止直接使用明文传输，禁止直接使用MD5、sha1等弱加密方式。 |
| 防暴力猜解 | 身份认证时，应防止暴力猜解账号口令： （1）在登录认证失败时给出通用的错误提示（如“账号或密码错误”），不能透露用户ID是否存在等信息。 （2）记录尝试次数，当超过阈值时（例如五次），限制访问（限制IP或锁定用户，锁定时间及解锁方式自行确定）。 （3）使用图片验证码防止暴力破解。 |
| Cookie安全性 | Cookie安全性 | 禁止将账号口令等敏感信息明文或简单编码存放在Cookie中。 |
| 访问控制 | 未授权访问 | 应建立安全的访问控制机制，禁止未登录用户访问用户登录后的资源、页面或URL。 |
| 防水平越权 | 重要操作（如转账交易、查询类操作、账号修改）时，系统应在服务器端对用户输入数据的合法性和有效性进行校验，防止水平越权（如用户A通过修改账号ID越权对用户B的账号进行操作）。 |
| 防垂直越权 | （1）授予不同账户为完成各自承担任务所需的最小权限，应严格限制默认账户或预设账户的权限，禁止将所有权限集中在某一预设账户上。 （2）在为用户授权时，服务器端按照权限规则对权限进行校验，互斥的权限不能共存于一人。如操作和审核权限。 （3）在重要操作（如账号增删改、授权、业务操作、业务审批）时，系统应在服务器端对当前用户的权限进行校验，防止垂直越权。 |
| 输入校验 | 防sql注入 | 应用系统应具有统一的防SQL注入机制： （1）防SQL注入输入校验，至少校验以下危险字符：select、 where、 from、and、or、union等。 （2）应使用存储过程或参数化查询，避免使用字符串拼接SQL语句，防止SQL注入。 |
| 防跨站 | 应用系统应具有统一的防XSS跨站校验攻击机制： （1）防跨站输入校验，至少应校验以下危险字符：< > " ' % ( ) & + \ \' \"，prompt，script， alert等。 （2）防跨站输出编码，如果数据是输出到HTML中则进行Html输出编码，如果数据是输出到javascript代码中进行拼接，则进行javascript输出编码。 （3）设置cookie的HttpOnly属性，能够有效防止XSS攻击。 |
| 文件上传 | 防止任意文件上传 | 应对上传文件进行以下处理，防止任意文件上传： （1）使用白名单方式控制上传文件的类型。服务器端应对上传文件的大小、扩展名、类型（报头信息）进行校验，防止任意文件上传。 （2）文件应尽量保存在文件服务器或web目录外部，避免通过web应用直接访问上传的文件。 （3）应控制文件上传目录的权限，禁止运行权限。 （4）应对上传文件进行重命名。 |
| 输入校验 | 应对上传文件中的所有参数字段（如文件名称、文件类型、其他信息等）进行输入校验，防止注入、跨站等漏洞。 |
| 数据安全 | 口令加密  存储 | 用户口令在存储过程中需进行加密，建议使用md5加盐(随机数)、sha2、pbkdf2等方式进行加密存储，禁止直接使用明文存储，禁止直接使用MD5、sha1等弱加密方式。 |
| 多余信息  返回 | 对服务器返回的参数做严格的限制，保证不是功能必须的参数不在返回的参数中，防止多余信息引起的数据泄露。 |
| 敏感信息显示要求 | 避免在html页面、js文件、客户端等前端上直接显示绝对路径、内网IP地址、账号口令等敏感信息。如： http://10.32.21.1/index.js; /var/www/html; user=admin,pass=admin; |
| 敏感数据  脱敏 | 敏感数据在显示时，应进行脱敏处理，如： 姓名：张三脱敏为\*三 身份证号：1002\*\*\*\*\*\*\*\*\*\*1237 手机号：186\*\*\*\*0781 银行卡号：623078\*\*\*\*\*\*\*\*\*4846 住址：\*\*\*\*3单元302 |
| 系统容错 | 统一错误  处理 | 应用系统应有统一错误处理功能，有效屏蔽系统技术错误信息，不将系统产生的错误信息（如中间件信息、数据库信息）直接反馈给客户端，提升用户体验，防止信息泄露。 |
| 框架安全 | 第三方组件或框架 | 组件和中间件是导致漏洞的重要原因，使用时需遵守如下要求： 1.使用的版本需是官方正常维护的版本，如不是最新版本，需更新当前版本的安全补丁或升级； 2.对使用的组件进行安全认证或限制源IP访问，避免造成未授权访问漏洞，如mongoDB、redis、Memcached、JBOSS、VNC、Zookeeper、Rsync、ElasticSearch、Hadoop、Kibana、Confluence、Jenkins、spring boot等； 3.登录各组件的默认口令需进行修改，修改要求参照口令安全策略，如REDIS、ES、ActiveMQ、RabbitMQ等； |

### 2.6 可扩展性需求

1）系统要求支持主流操作系统、数据库和通讯中间件，对软、硬件平台具有良好的可扩展能力，支持跨平台客制化开发；

2）支持交易数据导入、模型参数维护、计量、会计核算、报表模块对于新产品的支持，系统容易改进、扩展和升级；

3）提供的平台能够很好的实现业务功能扩展的灵活性，通过后台服务器对业务功能的模块化处理和可配置处理实现对功能的一站式更新，且不影响原有系统的正常运行；

4）系统的计算能力支持横向扩展；

5）对第三方平台提供良好的接口支持和扩展能力。

### 2.7 二次开发要求

为满足本行业务发展需要，系统应能灵活、方便、快捷地支持个性化需求开发，相关要求包括：

1）支持参数的个性化调整，从而适应监管要求及行内业务需求的变化；

2）支持数据采集范围扩展及接口快速开发；

3）支持较为便捷的全量/增量程序版本抽取和提交；

4）支持日常需求改造涉及的其他开发要求。

### 2.8 其它非功能性要求

2.8.1 运维要求

1）提供日常运行监控和完整的系统维护管理的方案：提供日志、实时交易监控等系统问题定位方案；提供日志和历史数据备份、清理机制；

2）系统日志需接入采购人智能运维平台，满足《重庆三峡银行应用日志规范》中的要求；

3）提供应用系统之间逻辑独立、启停服务时系统间不相互影响的部署方案（十分重要），保障系统的7\*24小时运行；

4）提供系统资源运行情况实时监控报告；提供系统出现异常预警报告；提供系统运行情况报表等；

5）涉及重大生产故障，需15分钟内响应，30分钟内提供临时解决方案并能恢复生产服务，并安排响应的技术专家进行技术支持。

2.8.2 日志要求

1）应完整记录所有通讯日志，如果通讯日志为字节码的，不能直接查看的，应提供查看工具；

2）应完整记录交易日志，方便交易统计分析，不同类型的交易可分不同的交易日志表；

3）可在线动态调整日志级别，在生产环境下定位问题时不需要中断服务；

4）系统相关日志应输出在应用目录之外；

5）不应在日志中记录客户支付敏感信息；不允许保留非本机构的客户敏感信息。

2.8.3 自动监控指标

1）磁盘占用率（关键目录）、CPU使用率、内存占用率等；

2）数据库连接池使用情况：总连接数、空闲连接数、使用中连接数；线程池使用情况：总线程、空闲线程、使用中线程；

3）虚拟机堆内存情况（适用Java）：空闲内存、使用中内存；

4）交易级的错误，应用系统重大错误。

### 2.9 应当遵循的标准和规范

应用应实现与行内各种操作系统、中间件、数据库、业务系统及工具软件进行平滑对接。系统的底层应支持各个层次的多种协议，支持与业务系统的互通、互联，应用系统采用标准的数据交换方式，保证数据共享。

系统架构必须遵循采购人应用架构统一架构规范；对外交互界面（含接口、交互流程）均需遵照采购人确定统一规范进行设计和开发；同时开发过程的产出物（如：设计文档、代码、测试案例、测试报告等）也需完全遵照采购人确定的统一标准规范完成。

业务处理符合国家法律、法规和有关政策规定。数据标准要满足银监会及人民银行相关管理办法及标准化的要求。

### 2.10 其他技术要求

1）开发环境基于J2EE轻量级框架，支持JDK版本：JDK1.8及以上版本。

2）操作系统、数据库和中间件等需满足信创基线要求，当前部分基线如下：服务端操作系统支持银河麒麟V10，支持OceanBase数据库，支持东方通内嵌中间件、Undertow中间件等。

3）必须支持Windows全系操作系统、银河麒麟桌面操作系统、MAC、IOS、Android、鸿蒙等终端操作系统。，支持谷歌、360、IE6及以上版本浏览器使用。

4）系统基础架构和底层数据库具备灵活性。

5）系统可高可用部署，支持负载均衡，具备横向可扩展性。

6）系统处理能力能够满足现有业务数据以及未来三年可能发展的业务数据量。

7）系统开发需要符合我行开发规范和整体框架要求。

8）系统需支持dns方式连接数据库以及应用。

9）原则上不对系统许可（license）做限制。

10）响应人需提供完善的数据备份方案及备份机制。

11）技术RTO（恢复时间目标）：2小时；技术RPO（恢复时间点目标）：1小时。

12）需支持IPV6协议。

13）禁止应用软件部署使用的安装码或授权码与其运行的基础环境（如：硬盘序列号、CPU序列号或网卡序列号等）进行绑定。

14）系统在集群部署共享文件访问时使用对象存储（不得使用NAS）。

15）满足国家保密标准及要求。

16）接入Devops研发效能平台，实现系统的统一的持续集成、交付、部署，确保符合《重庆三峡银行配置文件管理规范》等规范要求；接入Aiops智能运维平台，实现APM监控与日志中心的统一管理，确保符合《重庆三峡银行应用日志规范》及《APM监控采集兼容性及接入规范》等标准要求。

17）**实现当前已与现有即时通讯E-Mobile及时通讯单点登录集成的应用系统零开发、无缝切换到零信任安全平台。**

18）**零信任安全平台采用软件方案实现，以保障后期的可移植性。**

## **3.** 测试要求

1）响应人应负责系统的单元、集成和系统测试，提交完整的测试案例及达到准出标准的单元、集成和系统测试报告。

2）响应人应提供专职的性能测试负责人及性能测试人员进行系统的性能测试，提交满足系统性能指标的性能测试报告。

3）响应人应指派专职的测试项目经理及项目成员进行系统测试，参照采购人系统测试准入准出标准。

|  |  |
| --- | --- |
| **系统测试准入准出标准** | |
| **一、系统测试准入标准** | |
| **阶段** | **准入条件** |
| 计划阶段 | 开发项目在立项之初应提交纸质测试服务申请单给测试负责人 |
| 开发项目整体项目计划必须包含系统测试计划或系统测试计划时间 |
| 测试方要求的需求说明书及相关说明书已经通过评审，并形成终稿；文档包括但不限于：业务需求、需求说明书、系统原型、概要设计（可选）、用户手册（可选） |
| 变更影响范围是否提供 |
| 执行阶段 | 提交的产品经过了开发自测(单元及集成测试），并提交了测试案例与测试报告，单元及集成测试案例密度不低于20条/每功能点，案例需求覆盖度100%，无致命及严重遗留问题 |
| 系统测试案例准备就绪（案例密度为35条/每功能点） |
| 测试环境准备就绪 |
| 测试版本能够成功部署到测试环境。（如果测试和开发处于同一环境，则在系统测试开始前应该按照开发提交的版本重新部署） |
| 冒烟测试达到通过标准（冒烟测试案例通过率大于90%，有效缺陷率不高于10%） |
| **二、暂停/继续标准：满足下列之一的条件并由项目组审核同意，测试可以暂停** | |
| **序号** | **暂停条件** |
| 1 | 由于程序、环境原因导致测试无法进行 |
| 2 | 项目暂停，已无测试必要 |
| 4 | 测试需求稳定指数小于70%，则暂停测试执行 |
| 5 | 每个里程碑节点或执行轮次案例执行通过率低于60%，则暂停测试执行 |
| 6 | 每个里程碑节点或执行轮次缺陷解决率低于50%，则暂停测试执行 |
| 7 | 每个里程碑节点或执行轮次缺陷的案例命中率大于25%，则暂停测试执行 |
| 8 | 每个里程碑节点或执行轮次严重以上缺陷占比大于35%，则暂停测试执行 |
| 9 | 测试环境、测试数据、测试人员等等测试必备条件不再具备或发生变化导致测试不能进行，则暂停测试执行 |
| 10 | 项目组确定的可以暂停的其他条件 |
| 11 | 恢复以上的条件并由项目组审核同意，测试可以继续 |
| **三、系统测试准出标准：同时满足以下条件，系统测试完成** | |
| **序号** | **准出条件** |
| 1 | 测试需求覆盖率达到100%，测试案例覆盖度100% |
| 2 | 测试案例执行率达到100%，测试通过率95% |
| 3 | 缺陷修复率达到95% |
| 4 | 致命缺陷、严重缺陷解决率达到100% |
| 5 | 一般缺陷、微小缺陷解决率达到90%以上，建议缺陷解决率达到80%以上，且未解决缺陷得项目组认可 |
| 6 | 提交系统测试报告及通过评审 |
| **四、测试指标公式附录** | |
| **TPI** | **公式** |
| 测试需求覆盖率 | 测试需求覆盖点/软件需求功能点 |
| 有效案例总数 | 案例总数-无效案例总数 |
| 有效缺陷总数 | 缺陷总数-无效缺陷总数-伪缺陷总数 |
| 严重以上缺陷总数 | 严重及致命缺陷总数-无效的严重及致命缺陷总数 |
| 案例执行率 | 每轮执行案例数/每轮计划执行的案例个数 |
| 需求稳定指数 | （测试需求分析中规则数量-业务需求因素引起变更的测试需求规则数-开发因素引起变更的测试需求规则数）/测试需求分析中规则数量 |
| 案例执行通过率 | 每轮执行通过的案例个数/每轮执行案例数 |
| 缺陷的案例命中率 | 有效缺陷总数/有效案例总数 |
| 严重以上缺陷占比 | 严重以上缺陷总数/有效缺陷总数 |
| 缺陷解决率 | 关闭缺陷总数/有效缺陷总数 |

## **4.** 人员要求

1）响应人应承诺未征得我行书面同意的情况下不得更换项目成员。

2）所有成员必须为响应人单位员工，**响应人项目组成员须提供近半年公司为其缴纳社保的证明材料，不得外包其他单位员工。（员工参保单位为响应人或委托第三方公司代缴，均认定有效；若员工社保委托第三方公司代缴，需提供代缴材料证明与第三方签订的合同或协议。总公司参选的，分公司员工可计算入内，子公司不计算入内。分支机构参选的，总公司人员不计算入内。）【提供社保材料及相关证明材料】**

|  |  |
| --- | --- |
| 项目经理 | 主导过三个以上同类项目和具有五年以上项目经理工作经验，具有独当一面的技术能力；直接对项目的实施负责，通过对工期、成本、质量的控制（包括总体制定、执行、跟踪、调整相关计划，协调项目可用资源），确保项目按要求完成。 |
| 系统架构师 | 主导过三个以上同类项目和五年以上相关工作经历，并且熟悉SOA、分布式架构以及主流开发框架。 |
| 项目组开发人员 | 至少二年开发经验，开发组长须有至少五年开发经验，且均有银行相关系统的项目实施经历。 |

3）需提供人员简历信息，同时，采购人将对所提供的人员进行审核，达不到我行要求的将要求替换。项目经理及骨干成员须参加采购人组织的面试，面试人员在合同签订时不得进行更换。

4）项目组成员若有违约违规行为将由响应人承担责任。

## **5.** 项目实施要求

在本项目实施周期内，如遇到原系统功能与需求不符，需要及时调整实施方案，满足采购人的要求，并征得采购人同意方可变更。

响应人在项目实施过程中，需按照采购人项目管理规范提供相应文档（所有提交文档必须为中文）。

本项目为现场开发，原则上不允许远程开发模式，除非得到采购人的明确认可和授权。

## **6.** 项目源代码要求

本项目的所有源代码，包括产品源代码、客户化源代码、系统平台源代码及第三方产品源代码，底层架构和通讯层的源代码，代码解析平台（若有）及源代码说明文档、源代码注释说明、基线版本号等相关内容，除确实无法获取源代码的第三方产品外，响应人应进行无保留的知识转移。客户化源代码的知识产权归采购人单独所有，其余部分归双方共有。针对共有部分，采购人拥有在采购人及其分支机构使用及后续开发的权利，响应人拥有在其公司和其他组织范围内使用的权利，但响应人使用时不得侵犯采购人利益。

## **7.** 交付周期、地点

### 7.1 交付时间

2025年11月30日

### 7.2 实施及交付地点

重庆市。

## **8.** 验收测试

### 8.1 验收测试的范围

验收测试的范围为项目实施完毕,上线前最终确认的所有需求。

### 8.2 验收测试的组织

1）验收测试小组由采购人、成交供应商等有关人员组成，负责对项目建设进行验收测试。

2）成交供应商编制测试手册，经验收小组确认后，由验收小组负责验收测试。

3）在验收测试过程中，出现严重缺陷或质量问题时，验收小组可以决定暂停所有测试，直至缺陷和问题得到纠正。

### 8.3 验收测试的程序

1）对各功能模块进行测试；

2）在各功能模块测试合格的前提下，对系统进行全面初验；

3）系统验收测试合格后，进入试运行阶段；

4）系统在全行上线运行三个月后，进行验收。

### 8.4 验收测试的评定

测试结果按下列级别评定，并经验收小组签字认可：

•优良：功能和质量达到预期目的。

•合格：部分功能和质量不能满足采购人的要求，但成交供应商（集成商）采取了改正措施，使测试结果达到预期目的。

•不合格：功能和质量不能满足采购人的要求。

## **9.** 售后服务和支持

服务和支持的范围：

•系统的安装、部署和调试；

•项目的验收测试；

•项目的数据转换、数据迁移、模拟运行和试运行；

•与系统运行有关的技术问题（含操作系统、数据库、应用系统的整体性能调优等）

•项目上线后两年内，针对本项目的完善性需求以及监管提出的安全性需求，成交供应商需免费进行开发。

•相关技术及业务培训（其中在项目实施前必须组织技术人员进行平台二次开发培训，并提供平台的所有技术文档等）

•维保期以年度计算，应至少提供2年维保服务，维保服务起始日为验收后次日，维保服务期结束日需延期至到期当年的6月30日或12月31日中较近日期（即维保服务延期最长不超过半年）。

•响应人在响应文件中详细说明在系统维保服务期的具体服务内容，系统维保服务期过后有偿维保的内容、价格及收取方式，若按开发量评估收取，应说明每人/月价格；

**【响应人在响应承诺函中需对以上相关内容中进行阐述并作出相应承诺】**

## **10.**系统维保费用

维保服务期满后，每年维护费用不高于合同价8%，且每年系统升级改造工作量2个人月内不收费，具体维保费用以合同约定为准。

## **11.**文档和培训

### 11.1 文档

1）文档范围

包括成交供应商收集整理的系统建设中所形成的全部文字记载、录音和照片等，项目验收后由成交供应商向采购人提供。

2）文档内容

响应文件；系统总体规划书；系统需求说明书；系统详细设计说明书；系统源码；系统数据库设计说明书；系统使用和操作说明书；系统（含子系统）测试案例、验收方案；系统（含子系统）测试、验收报告；系统建设的详细工程日志；系统运行质量评估报告；系统变更和补充的相关文件、协议、录音、照片等。

3）要求

响应人提供的文档要保持完整性和准确性。所有文档都采用简体中文（第三方产品出厂文件除外）。

### 11.2 培训

1）培训人员

成交供应商应对下列人员进行相应的技术培训：

包括但不限于涉及本项目的相关开发人员、运维人员以及业务人员等。

2）要求

对所有的培训，响应人除提供完备的书面教材外，还应提交培训方案和计划。

采购人要求所有的培训在采购人指定地点进行。

## **12.**服务连续性预案

在本次询比中，响应人应在响应文件中提供服务连续性预案供采购人查看，服务连续性预案应考虑供应链风险产生的影响。【提供服务连续性预案】

## **13.**项目实施方案

在本次询比中，响应人应在响应文件中提供项目实施方案供采购人查看，方案应包括履行合同的时间计划、提交资料、人员安排等内容。【提供项目实施方案】

## **14.**付款方式

原则上不预付款项。本合同款项采用分期付款：

1）项目安装、调试并投入试运行后30个工作日内,乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总额的60％。

2）项目正式验收合格后30个工作日内, 甲方依据《服务水平协议（SLA）》对乙方服务质量作出评价，评价合格后，乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总价的30％，否则按《服务水平协议（SLA）》进行相应金额扣除。

3）维护到期后30个工作日内，甲方依据《服务水平协议（SLA）》对乙方服务质量作出评价，评价合格后，乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总额的全部余款，否则按《服务水平协议（SLA）》进行相应金额扣除。

## **15.**保密条款

### 15.1 保密范围

成交供应商在实施过程中接触到的采购人知识产权、经营信息等。

### 15.2 保密责任

双方互为保密资料的提供方和接受方，负有保密义务，承担保密责任。除经过双方书面同意，任何一方不得将有关内容提供给合同以外的第三人。

## **16.**报价要求

响应人应严格按照《响应文件格式》的“报价一览表”的格式认真填写。

## **17.**知识产权

成交供应商提供的产品和服务以及在项目中用到的各种工具、产品、组件、文档不得侵犯任何方的知识产权和其他合法权益。不得侵犯采购人商誉，任何人未经采购人同意不得使用采购人合法所有的知识产权，由此造成的一切损失由成交供应商承担赔偿责任。如无特殊说明，本项目定制开发部分知识产权归采购人所有。

一经发现成交供应商将采购人具有自主知识产权的系统代码违规转让、销售、赠送或泄露给第三方，或者通过互联网渠道（如百度网盘、GitHub仓库等）违规公开分享与该系统相关的重要配置数据、开发设计文档以及产品源代码，将视情节轻重情况给予成交供应商相应处罚（处罚金额不低于合同金额的10%）。

## 18.售后服务和培训方案

在本次询比中，响应人应在响应文件中提供售后服务和培训方案供采购人查看，方案应包括售后服务的内容、方案和计划，培训内容、方案和计划等内容。【提供售后服务和培训方案】

## **19.**其他

1）响应人必须在响应承诺函中对本章内容做出整体性响应和承诺，承诺内容必须达到本章及询比文件其他条款的要求。

2）响应人应根据本章内容和要求，提供对应资料，无遗漏。

3）其他未尽事宜由供需双方在合同中详细约定。

# 第四章 评审办法（综合评估法）

## 评审办法前附表

若评审办法前附表与正文不一致的地方，以评审办法前附表为准。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 条款号 | 评审因素 | 评审标准 | | |
| 1 | 评审办法 | 本次评审采用综合评估法。评审委员会按照评审办法前附表第2.1 条规定的标准进行初步评审，初步评审合格的响应人评审委员会按照评审办法前附表第2.2 条规定的评分标准进行打分，按得分由高到低顺序推荐1-3名成交候选人，但响应报价低于其成本的除外。综合评分相等时，以响应报价不含税低的优先；响应报价也相等的，由评审委员会按照响应人商务部分得分高的优先的原则排序。 | | |
| 2.1 | 初步评审标准 | 所有响应单位进行初步评审。初步评审内容：资格评审、形式评审、响应性评审。 | | |
| 2.1.1 | 资格评审标准 | 资格条件要求 | | 符合第一章“2. 响应人资格要求”规定 |
| 2.1.2 | 形式评审标准 | 响应人名称 | | 与营业执照、资格证明材料一致 |
| 响应文件的签字盖章 | | 符合第二章“响应人须知”4.6 条规定 |
| 响应文件的密封 | | 符合第二章“响应人须知”4.7 条规定 |
| 响应文件格式 | | 符合第六章“响应文件格式”的要求 |
| 响应文件组成 | | 符合第二章“响应人须知”4.2 条规定，内容齐全、无遗漏 |
| 联合体响应 | | 符合第一章“2. 响应人资格要求”2.5 条的要求 |
| 2.1.3 | 响应性评审标准 | 响应内容 | | 1. 在响应承诺函中对第三章“项目要求”内容做出整体承诺；  2. 根据第一章“2. 响应人资格要求”和第三章“项目要求”的要求规定，提供对应资料，内容齐全、无遗漏。 |
| 响应文件份数 | | 符合第二章“响应人须知”4.6 条规定 |
| 响应方案唯一 | | 只能有一个方案响应。 |
| 响应报价 | | 符合第二章“响应人须知”4.8 条规定 |
| 响应有效期 | | 符合第二章“响应人须知”4.4 条规定 |
| 响应保证金 | | 符合第二章“响应人须知”4.5 条规定 |
| 2.2 | 详细评审 | 分值构成与评分标准  (总分1OO分) | | 响应报价评分规则（分值：60分）  1.以各有效报价（不含税报价）之和的平均价格作为评审基准价，基准分为60分；  2.计算各有效报价与评审基准价的偏离度。偏离度=（有效报价/评审基准价-1）\*100%；  3.报价向上每偏离基准价的1%扣1分；扣完为止，不足1%的不予扣减；  4.向下偏离基准价10%以内的，不扣分；向下偏离基准价超过10%的，在向下偏离基准价10%的基础上，向下偏离每多超过1%扣0.5分，扣完为止，不足1%的不予扣减。 |
| 商务技术部分评分规则（分值：40分）  1、实施案例（分值：10分）  有效案例需同时满足以下条件：  （1）2022年1月1日至2025年1月1日（以合同签订日期为准）的国内国产化实施案例。  （2）案例须同时提供合同对应的发票之一及合同关键页复印件。  计分标准：  ①在响应人资格要求2.6中要求案例数基础上，每多1个SDP有效案例（合同内产品名称或建设内容包含“零信任(SDP)/软件定义边界(SDP)”中任意一个关键内容或字样）得0.5分，最多得2分。若本项提供的案例中包含银行案例，再得1分。  ②在响应人资格要求2.6中要求案例数基础上，每多一个IAM有效案例（合同内产品名称或建设内容包含“统一身份认证(IAM)/统一认证(IAM)/身份认证(IAM)/身份管理(IAM)”中任意一个关键内容或字样）得0.5分，最多得2分。若本项提供的案例中包含银行案例，再得1分。  ③在响应人资格要求2.6中要求案例数基础上，每多一个SDP和IAM整合建设的有效案例（合同内产品名称或建设内容既包含“零信任(SDP)/软件定义边界(SDP)”中任意一个关键内容或字样，同时也包含“统一身份认证(IAM)/统一认证(IAM)/身份认证(IAM)/身份管理(IAM)”中任意一个关键内容或字样）得1分，本项最多得3分。若本项提供的案例中包含银行案例，再得1分。  评审依据：合同关键页包括甲乙双方名称、双方印章、项目/产品的名称、合同/中标通知书签订时间等，国产化案例需在合同中体现适配国产数据库、中间件、国产操作系统等。合同对应的发票需同时提供网上税务系统查询发票截图（网上税务系统（https://inv-veri.chinatax.gov.cn/），查询发票截图应与合同发票数量及编码一致。发票应同时满足：开票日期晚于合同签订日期；发票购买方与合同买方一致；发票销售方与合同卖方（投标人）一致。  计分按有效案例的最高得分计分，不重复计分。  2、实施团队要求（分值：4分）  1）现场项目经理：具备信息系统项目管理师证书（高级）证书得0.5分；具有7年以上工作经验得0.5分，有10年以上工作经验得1分；具备重庆本地社保（提供响应截止时间前连续3个月社保证明），得0.5分。  2）现场系统架构师：具备系统架构设计师证书（高级）证书得0.5分；有7年以上工作经验得0.5分；  3）现场开发人员：具有7年以上工作经验得0.5分；具备重庆本地社保（提供响应截止时间前连续3个月社保证明），得0.5分。  注：参与本询比项目现场实施的项目组成员需要提供人员简历表（参考第六章响应承诺中项目组成员简历信息）。简历中相关资质证书需要提供证书复印件及网站查询截图，相关工作及项目经历需提供相应的证明材料，包括但不限于满足要求的案例合同中项目组成员名单，盖有合作方公章的证明材料等。工作经验年限需提供个人社保缴费记录。此处出示提供证明的人员必须作为本询比项目的项目组成员参与开发建设。  3、服务承诺（分值：25分）  本项目包含2年维保服务（维保服务期起始日为本项目最终验收后次日，维保服务期结束日需延期至到期当年的6月30日或12月31日中较近日期），维保服务期内每年系统升级改造工作量2个人月内不收费。维保服务到期后每年维护费用不高于合同价的8%。若维保服务期增加至3年且维保服务到期后每年维护费用降至不高于合同价的6%，得5分；若维保服务期增加至4年且维保服务到期后每年维护费用降至不高于合同价的4%，得10分。  （2）技术培训服务承诺（分值：5分）  响应人在《售后服务和培训方案》中承诺提供项目相关认证及培训，数量不少于40人次，认证人数不少于10人，得5分，本项满分5分。  （3）license授权（分值：10分）  license授权数量（license授权数量按人计算，最低要求3500）增加至5000，得5分；若对license授权数量不做限制，得10分。  4、认证要求 （分值：1分）  获得ISO9001（质量管理）、ISO20000（服务管理）、CMMI5级认证，得1分。 |
| 3 | 评审程序 | 1.初步评审前，按本章第3.1.3项的规定对响应报价有算术性错误的进行算术性错误修正。  2.评审委员会对响应文件进行初步评审。  3.初步评审合格的响应文件进行详细评审。主观评审部分由各专家独立评审打分，最后取平均得分，保留2位小数。  4.根据综合得分由高至低进行排序，推荐1-3家合格的成交候选人。并依次为第一、二、三成交候选人。 | | |
| 3.2.3 | | 响应人得分 | 响应人得分=响应报价得分+商务部分得分 | |

## 1. 评审方法

本次评审采用综合评估法。评审委员会按照本章第2.2 条规定的评分标准进行打分，按得分由高到低顺序推荐成交候选人，但响应报价低于其成本的除外。综合评分相等时，以响应报价低的优先；响应报价也相等的，由评审委员会随机抽取确定。

## 2. 评审标准

### 2.1 初步评审标准

2.1.1 资格评审标准：见评审办法前附表。

2.1.2 形式评审标准：见评审办法前附表。

2.1.3 响应性评审标准：见评审办法前附表。

### 2.2 分值构成与评分标准

2.2.1 分值构成：见评审办法前附表。

2.2.2 评审基准价计算方法：见评审办法前附表。

2.2.3 评分标准： （1）响应报价评分标准：见评审办法前附表；

（2）商务部分评分标准：见评审办法前附表；

## 3. 评审程序

### 3.1 初步评审

3.1.1 评审委员会依据本章第2.1 条规定的标准对响应文件进行初步评审。有一项不符合评审标准的，作否决响应处理。

3.1.2 响应人有以下情形之一的，其响应作否决响应处理：

3.1.2.1 有第二章“响应人须知”第9.条以及第11. 条规定的任何一种情形的；

3.1.2.2 有串通响应、弄虚作假等其他违反相关法律、法规行为的；

3.1.2.3 不按评审委员会要求澄清、说明或补正的。

3.1.2.4 本响应文件约定的其它情形。

3.1.3 响应报价有算术错误的，评审委员会按以下原则对响应报价进行修正，修正的价格经响应人书面确认后具有约束力。响应人不接受修正价格的，其响应作否决响应处理。修正原则见第二章“响应人须知”第4.9 条。

### 3.2 详细评审

3.2.1 评审委员会按本章第2.2 条规定的量化因素和分值进行打分，并计算出综合评估得分。

3.2.1.1 按本章第2.2 条规定的评审因素和分值对响应报价计算出得分；

3.2.1.2 按本章第2.2 条规定的评审因素和分值对商务部分计算出得分（评审委员会统一打分）；

3.2.2 评分分值计算保留小数点后两位，小数点后第三位“四舍五入”。

3.2.3 响应人得分=响应报价得分+商务部分得分。

### 3.3 响应文件的澄清和补正

3.3.1 在评审过程中，评审委员会可以书面形式要求响应人对所提交响应文件中不明确的内容进行书面澄清或说明，或者对细微偏差进行补正。评审委员会不接受响应人主动提出的澄清、说明或补正。

3.3.2 澄清、说明和补正不得改变响应文件的实质性内容（算术性错误修正的除外）。响应人的书面澄清、说明和补正属于响应文件的组成部分。

3.3.3 评审委员会对响应人提交的澄清、说明或补正有疑问的，可以要求响应人进一步澄清、说明或补正，直至满足评审委员会的要求。

### 3.4 评审结果

3.4.1 评审委员会按照得分由高到低的顺序推荐成交候选人。

3.4.2 评审委员会完成评审后，应当向采购人提交书面评审报告。

3.4.3 有效响应不足三个的，经评审委员会判定，响应人具有相对行业竞争力的，可继续进行评审并确定成交候选人。

### 3.5 对评审委员会成员的纪律要求

评审委员会成员不得收受他人的财物或者其它好处，不得向他人透露对响应文件的评审和比较、成交候选人的推荐情况以及评审有关的其他情况。在评审活动中，评审委员会成员不得擅离职守，影响评审程序正常进行，不得使用本询比文件没有规定的评审因素进行评审。

### 3.6 对与评审活动有关的工作人员的纪律要求

与评审活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透漏对响应文件的评审和比较、成交候选人的推荐情况以及与评审有关的其他情况。在评审活动中，与评审活动有关的工作人员不得擅离职守，影响评审程序正常进行。

# 第五章 合同模板

（本章节的合同条款及格式仅供参考，具体以合同签订时为准）

**编号：SXYH20220101018\_\_\_**

**重庆三峡银行**

**零信任安全平台项目合同**

**委托方（甲方）：重庆三峡银行股份有限公司**

**受托方（乙方）：**

**签订地点：重庆**

**目录**

[第一条 定义](#_Toc17203)

[第二条 项目名称、内容及要求](#_Toc15343)

[第三条 项目履行的进度、期限、地点、地域、方式](#_Toc3203)

[第四条 方案调整](#_Toc3357)

[第五条 验收](#_Toc3135)

[第六条 交付使用后维护期、系统完善和保修维护服务](#_Toc17464)

[第七条 技术辅导与培训](#_Toc5025)

[第八条 双方的权利、义务](#_Toc14621)

[第九条 乙方的声明与保证](#_Toc24688)

[第十条 知识产权](#_Toc27215)

[第十一条 第三方索赔](#_Toc14235)

[第十二条 保密](#_Toc4014)

[第十三条 价格与支付](#_Toc1407)

[第十四条 风险责任的承担](#_Toc12313)

[第十五条 违约与赔偿](#_Toc14742)

[第十六条 合同的解除](#_Toc14576)

[第十七条 合同变更及转让](#_Toc96)

[第十八条 争议解决](#_Toc20173)

[第十九条 通知与送达](#_Toc21949)

[第二十条 合同生效](#_Toc2294)

[第二十一条 不可抗力](#_Toc31521)

[第二十二条 反商业贿赂](#_Toc5451)

[第二十三条 附件](#_Toc30781)

[第二十四条 其他](#_Toc28866)

[附件一：工作（需求）说明书](#_Toc16916)

[附件二：项目人员名单及人员应急退出机制](#_Toc11394)

[附件三：验收标准及流程](#_Toc19835)

[附件四：维护服务条款](#_Toc31759)

[附件五：服务水平协议（SLA）](#_Toc11273)

[附件六：服务连续性预案](#_Toc22636)

**委托方: 重庆三峡银行股份有限公司（以下简称“甲方”）**

法定代表人：刘江桥

地址：重庆市渝北区嘉州路88号中渝国际都会4号写字楼

邮政编码：

联系人：

电话：

电子邮箱：

**受托方：XXXXXXXXXXXXX（以下简称“乙方”）**

法定代表人：

地址：

邮政编码：

开户银行：

账号：

税号：

联系人：

电话：

手机：

传真：

电子邮箱：

**鉴于：**

乙方具有良好的开发实施能力，甲乙双方经友好协商并达成一致，依据相关法律、法规的规定，就甲方委托乙方进行项目实施与技术支持，向乙方订购零信任安全平台项目的相关事宜订立本合同，以资信守：

第一条定义

在本合同中，除非有相反的表述，下列术语具有如下含义：

1.1“项目”系指乙方受甲方委托，单独为本合同目的依据合同附件一《工作（需求）说明书》的产品实施与数据迁移服务。

1.2“客户化工作”指项目交付乙方后乙方对甲方的需求进行开发实施。

1.3“产品实施数据迁移”指乙方产品的安装配置和业务数据迁移服务。

1.4“零信任安全平台功能”指乙方提供给甲方的附件一中所涵盖的平台功能。

1.5“缺陷逃逸率”：后一测试阶段测试期间发现的缺陷个数/（当前测试期间所发现的缺陷个数+后一测试期间发现的缺陷个数）。

1.6“试运行”：项目上线后进入试运行阶段，项目试运行至少3个月。在试运行期间，甲方随时将发现的逃逸的缺陷通知乙方，乙方在最快的时间内予以响应。

1.7“响应时间”：指乙方就甲方提出的问题予以答复的时间。

1.8“特别重大运营中断事件（I级）”：（1）由于重要信息系统服务中断或重要数据损毁、丢失、泄露，造成经济秩序混乱或重大经济损失、影响金融稳定的，或对公众利益造成特别严重损害的事件；（2）由于重要信息系统服务异常，在业务服务时段导致甲方两个（含）以上省（自治区、直辖市）业务无法正常开展达3个小时(含)以上，或一个省（自治区、直辖市）业务无法正常开展达6小时（含）以上的事件；（3）业务服务时段以外，重要信息系统出现的故障或事件救治未果，可能产生上述1至2类的事件。

1.9“重大运营中断事件（II级）”：（1）由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成严重损害的事件；（2）由于重要信息系统服务异常，在业务服务时段导致甲方两个（含）以上省（自治区、直辖市）业务无法正常开展达半个小时(含)以上，或一个省（自治区、直辖市）业务无法正常开展达3小时（含）以上的事件；（3）业务服务时段以外，重要信息系统出现的故障或事件救治未果，可能产生上述1至2类的事件。

1.10 “较大运营中断事件（III级）”：（1）由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成较大损害的事件；（2）由于重要信息系统服务异常，在业务服务时段导致一个省（自治区、直辖市）业务无法正常开展达半个小时（含）以上的事件；（3）业务服务时段以外，重要信息系统出现的故障或事件救治未果，可能产生上述1至2类的事件。

1.11“致命缺陷”：导致对被描述的主要对象的理解错误、不可行、不能运转、对业务和整个系统可能造成重大损失或损害。比如：（1）由于程序所引起的死机，非法退出；（2）死循环；（3）导致数据库发生死锁；（4）数据通讯错误；（5）严重的数值计算错误；（6）财务错误；（7）导致出现上述III级（含）以上事件；（8）对客户造成不利影响；（9）引起客户投诉；（10）对甲方声誉造成不良影响。

1.12“严重缺陷”：对被描述的部分对象的理解或实现错误，部分的系统或模块不可行或不能运转或部分系统和模块缺失，对整个系统有重大影响或可能造成部分的损失和损害。比如：（1）功能不符；（2）数据流错误；（3）程序接口错误；（4）轻微的数值计算错误。

1.13 “一般缺陷”：系统中部分单元模块或单个功能描述和实现有错误、有偏差、不一致或有缺失，不影响模块的正常运行，或有影响但可以有替代办法或避免办法。比如：（1）界面错误(详细文档)；（2）打印内容、格式错误；（3）简单的输入限制未放在前台进行控制；（4）删除操作未给出提示。

1.14 “微小缺陷”：基本不影响系统的运行和功能的实现。但是与标准、规范和定义不一致。比如：（1）辅助说明描述不清楚；（2）显示格式不规范；（3）长时间操作未给用户进度提示；（4）提示窗口文字未采用行业术语；（5）可输入区域和只读区域没有明显的区分标志；（6）系统处理未优化。

1.15“重大缺陷”：指严重缺陷和致命缺陷。

第二条项目名称、内容及要求

2.1项目名称：重庆三峡银行零信任安全平台项目

2.2项目内容、范围及要求

详细内容参考附件一《工作（需求）说明书》，最终以附件一中双方约定的内容为准。

2.3技术指标和质量要求。

见附件一、附件四。

2.4应当遵循的标准和规范。

乙方交付的零信任安全平台项目应当满足国家相关法律法规、监管政策和行业标准，需满足甲方各类内部管理要求，包括信息安全管理相关要求、客户信息保护相关要求、数据标准相关要求，涉及银联卡支付的需满足《银联卡支付信息安全管理标准》。

第三条项目履行的进度、期限、地点、地域、方式

3.1乙方必须投入足够的具有本项目实施能力的技术人员以保证本项目按期完成，乙方项目组主要成员及人员应急退出机制见附件二《项目人员名单及人员应急退出机制》，未经甲方事先同意，附件二中人员不得变更；如遇特殊情况需变更的，替换人员技术水平或级别需不低于被替换的人员水平或级别，并需通过甲方考察并取得甲方同意，否则甲方有权要求更换。

3.2进度：乙方应严格按照3.3所列示的期限完成项目实施任务。

3.3期限：上线时间为年月日前。

3.4地点：乙方完成项目实施工作的地点为：重庆；【驻场】实施。

3.5地域：本项目适用机构所在地域包括：重庆三峡银行总行各部门及辖内各经营机构。

3.6方式：

3.6.1协调：甲、乙双方各派出一名项目主要负责人负责本项目协调工作。其中，乙方代表负责提示完成本项目各阶段双方按照本合同应当履行的义务；经双方代表确认后分别与双方相关人员组织协调开展工作。

3.6.2 支持：乙方完成本项目有赖于甲方及时、全面、准确地向乙方提供需求信息和数据信息。同时，为完善项目需求，甲方亦有赖乙方针对性地提出建议性方案。甲、乙双方应当在上述方面给予对方必要的支持与协作，以保障项目实施工作顺利进行。

第四条方案调整

4.1因甲方原因提出导致增加【】∕人∕月以上工作量的需求变更，须通知乙方并由乙方确认，对此变更给乙方带来的额外劳动部分甲乙双方协商解决，由此变更导致项目进度延期不构成违约。但4.2款确认的，由乙方原因引起的工作量，甲方无需承担任何费用。

4.2 方案一经双方确认，任何一方有方案调整意见，均需与对方签字确认。

第五条验收

乙方负责的产品（即本合同2.2约定内容）在甲方生产环境正式安装部署（需遵循甲方系统上线相关的制度规范提交版本所需上线资料）完成后进入试运行期；上线试运行期间，本合同中的系统出现的任何问题，乙方应及时解决，保证试运行期间的稳定运行；试运行期间若出现较大运营中断事件（III级）及以上，乙方应予以立即解决，从出现中断事件至排除故障或解决问题期间的时间不计入试运行期，系统验收时间向后顺延。在符合甲方项目预期目标且试运行满三个月后，由甲方按照合同约定进行正式验收，验收通过后签署验收表或验收报告。

如果验收不合格，甲方有权另行指定正式验收的时间，在重新验收前乙方负责继续对项目进行修改和完善，并在甲方指定的期限内达到验收标准，其验收过程和方式不变。由此导致延误项目进度的，费用和责任由乙方承担，并按本合同第十五条之约定向甲方赔偿。再次验收仍不合格的，甲方有权解除本合同，不再支付任何费用。详细内容见附件三《验收标准及流程》。

第六条交付使用后维护期、系统完善和保修维护服务

6.1本合同金额包含【】年维护，维护期为自本产品正式验收合格后次日至次年并延期至6月30日或12月31日中较近日期（即维保延期最长不超过半年）。

6.2本合同产品的有偿技术服务期为本合同第6.1条约定的维护期到期之日起10年。本项目产品服务期内（包括本合同第6.1条约定的维护期与有偿技术服务期）如甲方对照附件一发现项目存在技术缺陷和隐蔽瑕疵，乙方应负责予以解决并应承担相应法律责任。

6.3乙方保证实施的项目产品在正常环境及状态下的正常使用和运行，且可与甲方原先使用的、本次被替代的系统兼容和无缝连接，不会导致甲方原使用的系统中数据和本项目应用后新的系统中数据丢失，若因乙方原因导致甲方原使用的系统中数据和本项目应用后新的系统中数据丢失的，甲方有权解除本合同，不再支付任何费用，且乙方应赔偿给甲方造成的损失。

6.4 维护服务期内（包括本合同第6.1条约定的维护期与有偿技术服务期）的服务内容和服务方式详见附件四《维护服务条款》。

6.5上述服务，不包括由下列事件引起的故障：

6.5.1 未能为系统提供适当的外部环境-如必要的系统环境、必要的管理体系、未能按照乙方要求配备资源等。

6.5.2 使用并非由乙方提供的产品或服务。

6.6在本合同第6.1条约定的维护期内，如甲方发现交付的项目、产品与双方最终签字确认的需求不符，尽管已经验收，但乙方仍具有立即纠正不符之处的责任。如乙方在收到甲方不符通知后 3 日内不到甲方现场进行检修，或在收到甲方通知后 10 日内仍不能纠正不符之处的，甲方有权采取其他措施（包括聘请第三方替代履行）以减少损失，由此产生的费用及相关损失由乙方负责。乙方承诺，甲方采取上述措施不必征得乙方事先同意，且不构成对乙方的任何侵权。

6.7 本合同第6.1条约定的维护期结束后的10年有偿技术服务期内，如甲方需要乙方提供维护服务,乙方应予提供。双方确认，甲方有权选择是否购买维护，乙方无权要求甲方对未使用维护服务的期间支付费用。

6.8 本合同并非维护期结束后的维护服务合同，有偿技术服务的合同由双方另行签订。

第七条技术辅导与培训

乙方应负责向甲方提供技术辅导与培训，以使甲方人员熟练掌握该项目产品的应用和日常维护。培训内容包括：对技术开发人员、系统管理人员进行系统部署培训、业务操作培训、运行维护培训、故障处理培训等。

具体培训内容由双方共同商定，并由甲方项目经理签字确认。

第八条双方的权利、义务

8.1除本合同其他条款外，甲方应承担如下义务：

8.1.1 按照本合同第十三条的规定向乙方支付报酬。

8.1.2 向乙方提供本合同约定的业务协作：如参与各方的资源协调与进度管理、商务保障、项目环境保障等，确保参与各方按期、按质协同工作。

8.1.3 指派一名项目主要负责人参加甲、乙双方为本项目召开的会议并协调相关工作和签署有关文件。

8.1.4 甲方为乙方解决现场人员正常开展工作的开发测试系统环境和场地。

8.2除本合同其他条款外，乙方应承担如下义务：

8.2.1 遵守法律法规及银行业金融机构内部管理制度及规定，贯彻执行相关监管政策。

8.2.2 按照本合同附件一的要求，采取一切必要的措施完成实施任务，保证项目的功能满足本项目需求，并确保在实施过程中严格执行版本过程化管理，配合甲方《软件研发项目实施细则》提供交付物。

8.2.3 负责在甲方的环境内安装并调试实施项目。

8.2.4 指派一名项目主要负责人参加甲、乙双方为本项目召开的会议并协调相关工作和签署有关文件。

8.2.5指派独立于开发团队的测试人员负责项目系统测试，并承诺按照甲方质量管理要求完成项目系统测试、性能测试、安全测试等。

8.2.6按照本合同的约定向甲方提供相关技术资料并提供技术指导。

8.2.7乙方需为甲方提供持续的项目风险识别和控制措施，并按甲方要求提供公司财务分析报告、项目进度报告以及重大事项报告等。

8.2.8 乙方应该适时开展风险管理评估和第三方审计工作，应该接受甲方的审核、评估以及外包检查，并配合接受来自监管机构的各项检查，配合对监管意见做出相应的管理、服务、基础设施、软硬件等整改。

8.2.9 乙方应针对服务内容为甲方制定业务连续性计划和应急计划并维护好相关资源，在服务质量不能满足合同要求时，甲方具有优先获取服务资源的权利。

8.2.10 乙方应当自己完成本合同项下的开发、测试或维护等工作，而不得分包给任何第三方，也不得进行转包或变相转包。

8.2.11 因政策或环境变化，或乙方由于其自身原因可能造成的服务变更或中断，乙方需配合甲方制定并按计划实施退出方案；过渡期间，乙方应继续履行约定的义务，保障甲方相关工作正常开展，保障业务连续性；并根据甲方要求，梳理项目可交付物，完成项目成果及资料交接。

第九条乙方的声明与保证

乙方向甲方做出如下声明与保证：

9.1乙方完全具有本合同项下项目实施的技术资质与实力，包括开发技术人员、硬件设施等。

9.2乙方已对照本合同附件一中甲方确认的需求，确认乙方的设计方案已经涵盖了设计需求的各方面，并且乙方实施的产品是先进的、适用的、兼容的，能够满足甲方核心业务扩展的需求。

9.3乙方在本项目中【使用/未使用】第三方产品，包括第三方SDK、小程序、软件、开源组件等，（若选择【使用】请列举）例：第三方SDK：XXXX、XXX；第三方小程序：XXX等。若乙方在项目中使用了第三方产品，乙方须按如下要求执行：

（1）针对第三方SDK：乙方应开展安全评估和个人信息保护评估，并提供无中高风险的评估报告；

（2）针对第三方小程序：乙方应开展安全评估，并提供无中高风险漏洞的安全评估报告。

（3）若第三方产品出现安全漏洞或违反个人信息保护相关法规，甲方有权要求乙方进行修复，若因此给甲方造成损失的，甲方有权随时向乙方追偿。

9.4乙方保证向甲方提供的项目产品（含第三方产品）的安全性、合规性，保证无恶意脚本、后门及恶意漏洞，不携带任何病毒，不越权收集、处理客户信息。

9.5乙方向甲方提供的产品和服务不会有任何第三方主张权利，也不会侵害任何第三方的合法权益，包括知识产权。

9.6乙方保证遵守甲方《重庆三峡银行员工回避管理办法》中招录回避、任职回避、公务回避的相关要求。若发现乙方人员与甲方内部人员存在亲属关系，乙方应主动报告，并采取相应回避措施。

9.7 乙方保证其人员无不良记录，服务商与其建立合法的雇佣关系，依法履行用工管理职责。

9.8 乙方定期通报外包事项，及时通报外包突发性事件及解决情况。

第十条知识产权

10.1乙方提供的产品和服务以及在项目中用到的各种工具、产品、组件、文档不得侵犯任何方的知识产权和其他合法权益。不得侵犯甲方商誉，任何人未经甲方同意不得使用甲方合法所有的知识产权，由此造成的一切损失由乙方承担赔偿责任，且甲方保留接触本合同，不再支付任何费用的权利。一经发现乙方将甲方具有自主知识产权的系统代码违规转让、销售、赠送或泄露给第三方，或者通过互联网渠道（如百度网盘、GitHub仓库等）违规公开分享与该系统相关的重要配置数据、开发设计文档以及产品源代码，将视情节轻重情况扣除乙方相应违约金（违约金金额不低于合同金额的10%）。

10.2 乙方行使任何基于本合同约定或法律规定取得的对软件产品的处分权，包括软件的转让权、专有使用权及使用许可权，都不得损害甲方基于本合同约定或法律规定取得的权利，也不得对甲方行使这些权利造成任何妨碍。

10.3乙方应将有关资料（数据库设计文件、技术文件和用户手册等全部资料）在甲方要求期限内，按国家有关项目开发标准以文字等载体的形式交给甲方，甲方拥有永久的使用权。乙方须提供全部源代码（包含以下内容：产品源代码、客户化源代码、系统平台源代码、开发平台、第三方产品源代码，底层架构和通讯层的源代码）、代码解析平台（若有）及源代码说明文档、源代码注释说明、基线版本号等相关内容，乙方应进行无保留的知识转移。

10.4本项目客户化源代码的知识产权归甲方单独所有，其余部分归双方共有。

10.4.1未经甲方事先书面同意，乙方不得将前述属于甲方知识产权的全部或部分转让给任何第三方，也不得进行任何形式的复制、改编、编译或衍生开发或者许可他人使用，包括将系统中有关甲方专有业务方式、业务流程规则、专有内容的技术实现方法等以任何方式用于任何第三方系统的设计及开发中。

10.4.2针对共有部分，甲方拥有在甲方及其分支机构使用及后续开发的权利，甲方在乙方交付的系统版本上进行自主开发或交由第三方公司开发，开发成果的知识产权归甲方所有。乙方拥有在其公司和其他组织范围内使用的权利，但乙方使用时不得侵犯甲方利益。

第十一条第三方索赔

11.1对于任何针对甲方提出的有关乙方提供的本项目产品的索赔，包括侵犯使用开发软件和资料或接受支持服务的国家的某项专利、实用新型、工业设计、版权、商业秘密、掩模图纸或商标的索赔，乙方应当自行与相关方协商解决并承担所发生的一切相关费用，负责承担甲方在索赔项下有可能产生的全部赔偿责任。

11.2对于第11.1条涉及的侵权索赔，乙方将承担全部费用，包括诉讼费、仲裁费、甲方支付的律师费、差旅住宿费、公证费、鉴定费、调解费及仲裁裁决、法院判决或调解协议中由甲方承担的赔偿金。

11.3如果产品可能引起索赔，乙方经甲方书面同意，并由甲方选择，采取下列补救措施：修改产品、取得任何必需的许可或更换产品。如果甲方认为上述任何方法不能实行有效补救，乙方应退还甲方已支付的全部款项并赔偿由此给甲方造成的全部损失。

11.4乙方对由以下非乙方的过错引起的侵权索赔不承担责任：

11.4.1 甲方使用不当所造成的侵权。

11.4.2 因甲方或第三方对开发软件或资料进行修改所直接造成的侵权。

第十二条保密

12.1乙方须对本合同项下的所有条款保密。乙方人员入场前须与甲方签订相应诚信安全承诺书。

12.2乙方应对本合同所述的客户信息、技术资料、业务流程、源代码、数据等重要信息采取保密措施，未经甲方的书面同意，乙方不得在合同允许范围外使用、披露、存放于第三方托管平台、向无关人员或第三方透露，也不能就有关合同内容的任何部分进行新闻的发布、公开的宣称、否认或承认。

12.3乙方不得以甲方名义开展活动，不得将甲方数据、信息以任何形式转移、挪用或谋取合同约定以外的利益。

12.4乙方知道违反本条规定将给甲方客户权利以及甲方造成难以弥补的损失，为此同意承担由此产生的经济上和法律上的责任和损失。

12.5乙方承认本合同中的技术资料和技术秘密为甲方所专有，将其对乙方进行披露并不意味着任何所有权、专利权的转让。

12.6在本合同项目的研究开发结束并通过验收后，乙方应向甲方提供本合同项目的研究成果，包括技术规范、测试文件和质量标准等相关的技术资料，或者计算机软件、文档及源代码等。乙方应归还甲方提供的所有技术资料或文件等，并承诺不保留任何复印件。

12.7乙方在下列情况下没有为任何信息保守秘密的义务，即当乙方已事先知道它无需为其保守秘密时；当该信息已为公众所知且不是由乙方未经授权而提供时；或者当乙方从某第三方合法地接受该信息且没有保密限制时。

12.8除非甲方特别声明，乙方对于保密信息的保密义务为无限期保密，直至甲方宣布解密或者保密信息实际上已经公开。

12.9 本合同项下乙方人员行为视为乙方行为，乙方应承担全部责任及损失。

第十三条价格与支付

13.1本项目合同总金额（价税合计）为\_\_\_\_\_\_\_元（大写：整），不含税价为：\_\_\_\_\_\_\_元（大写：整）,税额为：\_\_\_\_\_\_\_元（大写：整）。其中产品金额（价税合计）为\_\_\_\_\_\_\_元（大写：整），实施金额（价税合计）为\_\_\_\_\_\_\_元（大写：整）。不含税价格不因国家税率变化而变化，若在合同履行期间，如遇国家的税率调整，则价税合计应相应调整，以开具发票的时间为准。该金额为本合同约定项目的全部费用，除双方另有约定外，甲方无须向乙方支付其他任何费用。

本项目产品价格（含实施金额部分）如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **产品名称** | **模块** | **单价（元）** | **数量（套）** | **金额小计（元）** |
|  |  |  |  |  |
|  |  |  |  |
| 合计（含税） | 大写（人民币）：元整 | | | |

13.2支付方式：

本合同款项采用分期付款：

13.2.1项目安装、调试并投入试运行后30个工作日内,乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总额的60％，即元（大写：元整）。

13.2.2项目正式验收合格后30个工作日内, 甲方依据附件五《服务水平协议（SLA）》对乙方服务质量作出评价，评价合格后，乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总价的30％，即元（大写：元整），否则按《服务水平协议（SLA）》进行相应金额扣除。

13.2.3本合同第6.1条约定的维护到期后30个工作日内，甲方依据附件五《服务水平协议（SLA）》对乙方服务质量作出评价，评价合格后，乙方向甲方提供合法足额的增值税专用发票，甲方向乙方支付合同总额的全部余款，即元（大写：元整），否则按《服务水平协议（SLA）》进行相应金额扣除（13.2.2中已扣除部分，本条不重复扣减）。

13.3发票要求：

乙方须严格按照合同内容开具税率为6%的增值税专用发票（若遇国家税率调整另议），乙方在甲方每次付款前30个工作日需向甲方交付合法足额发票，否则甲方有权拒绝支付任何费用且不承担逾期付款违约责任。

第十四条风险责任的承担

14.1在履行本合同的过程中，确因在现有技术水平和条件下无法克服的技术困难，乙方应及时与甲方共同协商解决方案，若乙方没有及时通知甲方并采取措施导致研究开发部分或全部失败所造成的损失，风险责任由乙方承担。

14.2乙方发现可能导致实施项目失败或者部分失败的情况时，应当及时通知甲方并采取适当措施减少损失；乙方没有及时通知甲方并采取适当措施致使损失扩大的，应当就扩大的损失承担责任。

14.3若乙方由于公司经营决策重大变故、重要资源调整或是其他原因导致无法完成合同约定的开发内容，或乙方开发成果中的软件在安装、使用过程中发现由乙方原因造成的缺陷或瑕疵的，乙方应在接到甲方通知后予以解决或修复；若乙方无法解决，或者拒绝解决或修复，可由甲方委托第三方进行处理，但由此发生的费用由乙方负担；如因此给甲方造成损失的，乙方还应当赔偿甲方因此遭受的损失。

第十五条违约与赔偿

15.1因甲方原因未按本合同规定支付第一期款项，且经乙方合理催告后，仍无正当理由并逾期支付达【30】个工作日以上的，乙方有权解除合同。

15.2因甲方原因逾期支付第二期或第三期款项的，自逾期一个月后的第二天起，每逾期一天支付应付逾期付款金额的万分之五的违约金，违约金总额不超过应付款额的20%。

15.3乙方未按计划或不实施研究开发工作，甲方有权要求乙方实施研究开发计划并采取补救措施。如乙方逾期一个月仍未按计划或不实施研究开发工作，甲方有权解除本合同，并且乙方应在10个工作日内返还所有甲方提供的报酬，返还或销毁甲方提供的有关技术资料和文件，并承担本合同总额20%的违约金。

15.4乙方应按本合同规定的研究开发进程完成开发项目。若因乙方自身原因未按时完成开发项目，则按照附件五《服务水平协议（SLA）》扣除延期违约金。

15.5乙方未能完成甲方委托的开发项目或开发成果不符合本合同约定的要求，乙方承担本合同总额20%的违约金，并返还甲方已支付的费用。

15.6乙方将甲方支付的费用于履行合同以外的目的，甲方有权制止并要求其纠正。如因此造成本合同项目停滞、延误或失败的，乙方应当承担给甲方造成的损失赔偿责任。

15.7除本条、附件五《服务水平协议（SLA）》及其他条款另有约定外，乙方违反本合同任一条款的，应向甲方支付合同总额5%的违约金并赔偿甲方产生的损失。

15.8本合同项下乙方应支付的违约金、赔偿金等，甲方均有权从应支付给乙方的款项中优先扣除，若有不足，乙方应另行筹措资金补足。

第十六条合同的解除

16.1如果满足以下条件，任一方在通知对方后，都可以解除本合同。

（1）一方严重违反本合同项下的义务，并且违约方在对方通知后三十天仍未纠正，非违约方向违约方发出解除合同的书面通知时。如果该违约无法在三十天内纠正，而违约方在此期限内已经开始着手，并将以努力诚恳继续纠正此违约行为，则守约方应为违约方合理地延长该时间的期限。

（2）当一方按正常程序停止经营业务、破产、处于付款拖欠、延期偿付、公司重组或倒闭状况，或全部转让利润与债权人、书面承认无力偿还到期债务、委派清算人清算其业务或财产。

16.2除本合同约定的情形外，甲方若认为乙方无法胜任本合同项下工作的，有权随时通知乙方后解除本合同。甲方除据实与乙方结算费用外，不承担其他违约责任。

16.3当本合同以任何原因解除或终止时，乙方应将本合同项下的过程文档、资料等全部交付给甲方，配合甲方完成知识转移，保证甲方能够继续开展工作；乙方应立即停止使用并销毁包含甲方机密信息的所有物件，并证明该销毁情况；或者将这些物件归还给甲方。

第十七条合同变更及转让

17.1对本合同及其附件的内容进行变更，必须经双方协商一致并签订补充协议，方能生效，本合同另有约定的除外。

17.2本合同双方在未取得对方事先书面同意的前提下，均不得将各自本合同项下的任何权利或义务转让给第三方。

第十八条争议解决

本合同的解释、效力、履行及其他事项，均适用中华人民共和国法律、法规，如无法律、法规规定，适用有关行政管理部门规章。本合同履行中双方发生任何争议，应协商解决，协商不成的，任何一方均可向重庆仲裁委员会按照该会届时有效的仲裁规则申请仲裁，仲裁裁决是终局性的，对双方均有约束力。

第十九条通知与送达

除双方另有约定，本合同项下的所有书面通知，按本合同首部载明的地址及联系方式进行，乙方地址、联系方式如有变动，应于10日内以书面形式通知甲方，甲方地址、联系方式如有变动，应采用公告、网上银行、电话银行等方式通知乙方。否则，向本合同首部载明的地址和联系方式发送有关文件，均视为送达。

发生纠纷的，本合同首部载明的地址为司法送达地址，法院、仲裁机构等有权机关依照前述地址邮寄的传票、证据、通知、裁定、判决等诉讼（仲裁）文书及执行阶段法律文书资料，无论是否签收，均视为送达，当事人承担法律责任。

第二十条合同生效

本合同自下列条件全部满足之日起生效：

双方对本合同及其全部附件内容达成一致并加盖公章。

第二十一条不可抗力

21.1不可抗力是指本合同生效后，发生不能预见并且对其发生和后果不能防止或避免的事件，如地震、台风、水灾、火灾、战争、传染病等，致使直接影响本合同的履行或不能按约定的条件履行。

21.2发生不可抗力的一方应立即通知对方，并在十五天内提供不可抗力的详情及将有关证明文件送交对方。

21.3发生不可抗力事件时，甲乙双方应协商以寻找一个合理的解决方法，并尽一切努力减轻不可抗力产生的后果。

21.4如不可抗力事件持续三十天时，甲乙双方应友好协商解决本合同是否继续履行或终止的问题。

第二十二条反商业贿赂

乙方不得对甲方或甲方任何员工有任何商业贿赂的行为，否则经查证属实后，乙方应对甲方赔付相当于合同总额50%的赔偿金。该条在法律允许的范围内，不受任何免责或限制责任的条款制约。

第二十三条附件

本合同的附件与合同正本具有同等法律效力，主合同与附件如有冲突，以主合同为准。本合同附件如下：

附件一：工作（需求）说明书

附件二：项目人员名单及人员应急退出机制

附件三：验收标准及流程

附件四：维护服务条款

附件五：服务水平协议（SLA）

附件六：服务连续性预案

第二十四条其他

24.1除本合同另有约定之外，本合同约定的权利、补救和特权具有累积性，并不排除中国法令规定的任何权利、补救和特权。任何一方没有行使其权利或没有就违约方的违约行为采取任何行动，不应被视为是对其权利的放弃或对追究另一方违约责任权利的放弃。任何一方放弃针对违约方的某种权利，或放弃追究违约方的某种责任，不应视为对其他权利或追究其他责任的放弃。

24.2双方确认，已详细阅读过本合同及附件，并同意本合同及附件为甲乙双方所有约定的全部记载，替代双方在此之前或执行本合同过程中所做的任何书面或口头的交流、声明或协议。如果由于任何原因使本合同下的任何条款或内容成为无效或被依法撤销，本合同其他条款或内容的合法性、有效性和可执行性不受影响。

24.3本合同签订后，如需要就与合同执行有关的事项签订补充合同，应由双方加盖公章后，补充合同即生效。本合同附件为本合同的组成部分，本合同与附件如有冲突，以本合同为准。

24.4本合同以中文版本为准，除非本合同明确规定或双方另有约定，为履行本合同的所有文件及信函均以中文书写。

24.5本合同一式肆份，甲方执贰份，乙方执贰份，每份具有同等法律效力。

**（以下无正文）**

甲方：**重庆三峡银行股份有限公司**（公章）

乙方：**XXXXXXXXXXXXXXXX公司**（公章）

日期：年月日

附件一：工作（需求）说明书

1.1 需求概述

基于零信任理念的新一代安全办公体系建设，通过零信任SDP（SDP：Software Defined Perimeter）、统一身份认证（IAM：Identity and Access Management）和即时通讯（IM：Instant Messaging）等模块，构建全新的安全办公体系解决方案，以提升安全防护能力，满足合规要求，并优化用户体验。

（1）构建动态灵活的零信任SDP。零信任SDP根据用户信息、设备状态、地理位置、时间窗口、设备特征（如要求安装并开启了指定的杀毒软件才能接入）、用户行为等因素，实现了多维度的精细化管理，使访问策略可以精准细化到每个独立个体，最小化潜在的风险面。每个请求都经过严格的验证和授权过程。对外部隐藏内部网络结构和敏感服务，只有通过SPA（Single Packet Authorization）单包认证后才能建立连接，减少攻击面，而不是传统基于网络边界的控制列表ACL（Access Control List）,提升资源访问的安全性，增强策略的灵活性，更好地适配多样化的业务需求。

零信任SDP模块提供了一个安全的接入环境，利用基于身份的访问控制和权限认证机制，让内部应用和服务“隐身”。当黑客试图进行攻击时，会发现看不到目标而无法攻击，只有获得权限的业务人员可以正常访问，确保内部资源不受外部威胁，同时通过持续的身份验证和设备检查实现主动防御能力。降低潜在的安全风险，增强整体的安全性。

（2）建设统一身份认证IAM。为人员身份、认证、授权的全场景提供基础服务，涵盖身份管理、统一认证、多因素认证（MFA）、认证风险控制、权限控制及身份管理与认证审计。通过这些功能，IAM集中管理和维护所有用户的身份信息，确保数据的一致性和准确性，形成用户统一身份信息，实现从入职到离职的全生命周期管理。

作为零信任安全架构的核心，IAM以身份ID为中心构建身份认证管理系统，将用户身份作为重要的安全防护要素。系统默认对用户身份“不信任”，持续认证用户身份，并根据实时行为动态调整访问权限。IAM通过持续检测用户行为风险，提供多系统间的单点登录（SSO）体验，又保障访问的高安全性。

（3）打造零信任防护的即时通讯IM。在零信任建设中，构建一个以IM为入口的办公APP，覆盖消息、协同办公、任务管理、互联互通等多层面功能的一站式平台。该平台将内部系统与应用整合为卡片式设计，融入即时通讯工作台，成为员工的统一办公入口。

通过集成零信任SDP SDK，减少终端侧APP的数量，提供了安全沙箱能力和细粒度的数据安全控制（如应用只能在APP内打开、只能在线查看、防截屏、敏感信息脱敏展示等能力），从而简化操作流程，提高协同效率，使员工只需通过即时通讯界面即可便捷访问所有应用与服务，构建一个高效、安全且易用的办公工作台。

**本项目通过复用现有的OA系统自带的即时通讯E-Mobile软件进行优化集成**。通过对现有即时通讯E-Mobile软件性能优化和安全升级，作为员工便捷访问所有应用与服务的统一入口，提升整体办公平台的效率，满足企业对数据安全、统一管理和用户体验的高标准要求。

1.2 功能要点

主要功能如下表所示：

|  |  |  |
| --- | --- | --- |
| 零信任SDP | 控制中心 | 控制中心部署在企业的内部私有服务器上，通过管理平台，管理员可以管理和查看，主要功能包括：零信任办公策略管理、全网终端资产管理，安全策略管理，管控策略管理，安全准入管理、数据防泄漏管理、日志审计管理等。 |
| 零信任接入网关 | 部署在互联网及内网可达区域，以便互联网终端、内网终端均可无障碍访问无边界接入网关，从而顺利访问企业后端业务系统。控制中心及无边界网关，均可支持高可用部署架构，并可根据实际业务访问量及并发负载，进行水平扩展，保证访问企业后端业务系统的连续可用性。 |
| 终端零信任接入 | 在终端上为用户提供零信任接入入口 |
| 终端管控 | 提供终端管控等功能，支持Win、Mac、Linux、Android、IOS、鸿蒙操作系统终端安全检测能力。 |
| 水印保护 | 支持对终端设置屏幕及打印明、暗水印，对于截屏、拍照等泄露方式可追溯查找泄露源 |
| 统一认证平台（IAM） | 统一身份 | 机构管理、角色管理、凭证管理、自助服务等 |
| 统一认证 | 提供通用目录服务、域认证、应用SSO、认证管理、会话管理、多因素认证（MFA）等 |
| 统一权限 | 权限建模、平台权限、权限合规等 |
| 监控预警 | 访问时间、地点、设备、黑白名单、风险策略等 |
| 合规审计 | 账号审计、登录审计、操作审计、访问审计、认证审计等 |
| 移动办公安全防护 | 数据安全 | 实现APP内隔离的安全工作空间、安全水印、防截屏、打印管控等功能，实现存储、网络、应用、外设等隔离，形成端、网、业务、文件、数据的全周期访问控制闭环，解决数据落地泄漏问题，保障数据全生命周期安全。 |
| 工作台安全 | 为工作台的单点登录应用系统提供统一的零信任安全防护，实现单点登录系统零改造。 |

1.3 核心要点详细信息

|  |  |
| --- | --- |
| 功能分类 | 详细描述 |
| 身份管理 | 1. 组织管理：支持定义多套组织维度，自定义组织属性（如名称、编码、描述等），以树形结构展示组织，可扩展组织属性。具备组织查询、新增、删除、修改、迁移、合并、排序功能，能设置组织岗位范围和默认岗位，支持组织导入导出。 |
| 2. 组织模型管理：支持定义多套组织维度，每个维度下可自定义组织属性（唯一性、必填性、可见性、显示顺序等），通过正则表达式与字典约束属性内容，可灵活调整组织机构及所属人员。 |
| 3. 用户管理：支持自定义用户类型（内部用户、外部用户、临时用户等），每个用户类型可自定义用户属性（如姓名、性别、联系方式等）。以树形组织用户结构呈现，支持用户查询、新增、删除、修改、迁移、排序、设置主副部门、设置岗位、导入、导出操作。 |
| 4. 用户模型管理：支持自定义多种用户类型，每个用户类型可对用户属性进行详细设置（是否唯一、必填、管理员是否可见、用户是否可自助编辑、显示顺序等），支持正则表达式与字典约束属性内容，以及属性脱敏配置（如手机号、身份证号脱敏）。 |
| 5. 用户组管理：支持用户组新增、删除、修改、查看。可按部门、人员及规则添加用户到用户组，规则包括定义多个分组策略（分组策略内条件为与关系，分组策略间为或关系），支持按部门范围、部门属性（等于、不等于等多种匹配规则）、用户属性（等于、不等于等多种匹配规则）定义分组策略，支持添加人员到用户组，支持用户自动分组策略排除用户管理（排除用户不受自动分组策略影响，可查看、修改）。 |
| 6. 数据源同步：支持通过 LDAP 拉取、DB 拉取、FTP 拉取、API 拉取、API 推送、Excel 初始化等方式，从企业微信、钉钉、飞书等办公平台通过标准接口同步数据，整合企业零散的组织用户数据，形成权威的组织用户体系，根据不同应用所面向的用户进行按需同步。 |
| 7. 数据源同步流程装配：支持配置身份数据同步过程中的处理事件动作，涵盖从上游身份源到 IAM 平台数据，再到下游应用的整个流程，流程分为数据预处理（数据传入 IAM 平台，落入数据库前的处理动作，如数据预调整）、事件动作（数据落入数据库未提交时的处理动作，同步任务，失败则数据回滚）、任务动作（数据成功落入数据库提交后的处理任务，异步任务，按 IAM 平台调度执行）三个模块。 |
| 8. 身份集成配置：支持把平台组织、用户、岗位、自定义对象等数据同步给下游应用系统，支持定义多个应用系统数据同步策略，可通过 API 拉取、API 推送、LDAP 推送、FTP 推送等方式进行配置。 |
| 9. 用户密码策略：支持用户默认密码策略、用户随机密码 + 通知策略。可配置是否启用强制修改初始化密码策略、密码有效期策略（设置密码有效期、过期提醒时间、过期强制修改时间、提醒方式）、历史密码检测策略（用户不能使用最近三次历史密码作为新密码）、弱密码检测策略（开启时对用户修改密码等场景检测，支持弱密码库管理与规则定义）、自定义密码复杂度策略（以及根据用户、用户组设置）、密码策略白名单管理（加入白名单用户不受多种密码策略限制）、AD 密码反向同步策略（保证 AD 与 IAM 用户密码一致性），可按用户类型、指定用户、组织机构、自定义范围（用户属性）条件分别进行密码策略配置。 |
| 10. 用户数据同步：具备业务侧与网络侧的用户数据同步能力，在统一身份认证功能中创建或删除组织和用户后，零信任功能中相应数据应同步创建或删除，实现统一的组织和账号管理。 |
| 应用管理 | 1. 应用信息管理：支持管理接入系统的各类应用（BS 端应用、CS 端应用等）基础信息。应用管理界面支持按应用名称、应用分类、应用形态、应用认证协议筛选应用，应用列表显示应用名称、图标、形态、认证协议、分类、状态、创建时间、修改时间，支持应用的创建、编辑、删除、查看详情操作。 |
| 2. 应用授权管理：支持接入系统导入授权，以及按照用户组、用户进行授权。应用授权界面可查看应用授权详情（用户姓名、账号、授权来源），支持导入应用授权、授权应用给用户和用户组。 |
| 3. 应用账号管理：支持应用自定义账号策略和身份即账号策略，允许管理员对应用组织与账号进行管理，提供应用账号自动生成策略、存量应用账号自动绑定用户策略、用户通过门户绑定自助绑定应用账号策略。实现灵活的应用账号管理，包括分配、锁定、回收、停用等管理，一人多账号场景管理，孤儿账号管理，公共账号管理，支持设置长期未使用的账号为闲置账号（可自定义闲置账号时长，支持自动或手工禁用闲置账号）。 |
| 4. 应用数据同步：具备业务侧与网络侧的应用数据同步能力，在统一身份认证功能中创建或删除应用后，零信任管理平台中相应应用应同步创建或删除，实现统一应用管理。 |
| 认证管理 | 1. 认证协议管理：支持多种认证协议，BS 端系统单点登录支持 Cas、Oauth、OIDC、SAML、JWT、RADIUS、RESTFUL、PORTAL 等协议及密码代填，提供 SDK 供应用系统快速集成；CS 端系统单点登录支持 Oauth 协议与密码代填；移动端免密认证支持 Android、iOS、H5 移动应用形态，支持 Scheme 唤起、集成 SDK 唤起、APP 微门户；支持 Radius、LDAP、tacacs + 认证协议，支持 802.1X 以及 portal 认证协议。 |
| 2. 认证源管理：支持多种认证方式（密码认证、扫码认证、动态口令认证、短信认证、邮箱认证、消息认证、推送认证、临时授权、人脸认证、CA 认证、AD 域认证、第三方认证等），每种认证方式可配置不同的认证源。支持创建多个外部 AD/LDAP 认证源、外部 API 密码认证源，数据源同步时指定用户密码认证源，管理员可切换用户密码认证源；扫码认证支持认证 APP 扫码、多个企业微信 APP 扫码等多种 APP 扫码及多码合一技术；动态口令认证支持认证 APP 在线令牌、企业微信小程序令牌等多种令牌；消息认证支持通过企业微信、钉钉、飞书消息通道发送验证码进行认证，支持设置多个消息通道，实现消息通道合一，平台智能识别用户消息通道；第三方认证支持创建企业微信、钉钉、飞书认证源用于单点登录，支持创建基于标准认证协议的第三方 IDP（标准认证协议支持 Cas、Oauth、OIDC、SAML、JWT）。 |
| 3. 认证策略管理：支持登录策略和访问策略。登录策略可按应用、网络、时间、用户行为因子设置访问控制策略（如配置会话有效时间、登录失败锁定次数、登录页有效期、密码到期提醒、控制策略优先级、用户禁用状态监测、用户锁定状态监测等全局策略）；访问策略可按用户、用户组、应用、应用账号、网络、时间、用户行为因子设置访问控制策略，访问控制策略支持提升认证（执行认证级别、执行认证方式）、拒绝登录。 |
| 4. 认证设备管理：支持对移动认证设备和 PC 设备进行管理，可查看设备信息（用户账号、设备名称、操作系统版本、设备指纹、设备风险、设备状态信息），支持对设备进行删除、锁定、解锁操作。 |
| 5. 单点登录联动：具备业务侧与网络侧的单点登录联动能力，实现应用门户单点和业务应用单点登录。通过零信任客户端，在统一身份认证功能中创建应用并授权给用户，在零信任功能中创建统一门户应用并授权给用户，用户登录零信任客户端后可直接单点访问授权应用。 |
| 权限管理 | 1. 多种权限模型：支持 RBAC、ACL、DRBAC、ABAC 等多种权限模型，可根据应用系统情况选择配置，设置具体参数（如角色、权限对象等），提供属性定义（权限对象、数据字典等编辑与添加操作），可设置权限授权有效期与权限申请有效期。 |
| 2. 应用权限体检：支持权限检查功能，能够展示系统中未授权账号、违反互斥账号、敏感权限账号、相似角色、静默角色、静默功能权限、静默数据权限，选中其中一项能够跳转查看具体账号权限情况。 |
| 3. 权限合规检测：支持权限合规检查与敏感权限管理能力，可设置合规规则、互斥规则（系统互斥、角色互斥、菜单互斥以及行为互斥）、业务角色互斥（业务角色互斥与业务系统角色互斥），进行规则扫描，查看用户合规审计与应用合规审计，提供敏感权限管理（包括角色、菜单权限、按钮以及数据权限）。 |
| SDP - IAM 联动 | 零信任平台与统一认证平台（IAM）无缝对接，从 IAM 同步账密、机构、应用等数据及状态信息（如禁用状态、绑定状态），自动同步 IAM 用户与应用的授权关系，在应用门户展示用户可访问的应用（与 IAM 中相同用户权限一致），简化运维流程。 |
| 终端管理 | 1. 终端分类管理：支持提供设备动态分类以及设备管理的能力，可添加设备分类策略（如企业设备分类策略：【终端在域中】AND【终端运行任意一款杀毒软件】；僵尸设备分类策略：设备超过 1 天不活跃；未命中以上分类策略的设备均为 BYOD 设备）。可查看不同分类设备信息，对设备执行强制注销操作，不同分类设备登录客户端后展示不同信息。 |
| 2. 终端设备激活：支持提供灵活判断终端设备绑定方式的功能（一对一、一对多绑定等），为注册成功终端设备颁发可信设备身份。可创建多种设备绑定策略（如企业设备自助绑定策略、企业设备人工审批策略、BYOD 设备人工审批策略、BYOD 设备禁止绑定策略），根据不同条件（终端是否在域中、是否运行杀毒软件、客户端 IP 等）设置绑定方式（自主绑定、人工审批、禁止绑定），在绑定登录过程中，客户端有相应提示，管理员有审批通知并可进行审批。 |
| 3. 终端准入策略：支持提供持续检测终端环境及终端合规、准入控制的能力。通过零信任客户端采集不同操作系统 PC 环境（高危端口、运行的软件、零信任客户端版本、运行的杀毒软件等）和移动端环境（操作系统版本、零信任客户端版本、系统是否被 ROOT / 越狱等）信息，对 PC 端访问应用进行可信标记，基于终端安全状况和访问进程进行访问控制（如设置系统版本基线策略、合规进程基线策略、风险策略等，根据策略进行安全警告、禁止登录、二次认证等操作）。 |
| 4. 终端限流访问：支持对接入服务进行流量并发保护，下发终端限流策略（如新建限流策略，包括直接转发限速、隧道传输限速，超过速率客户端执行丢弃策略），配置 SDP 服务限流策略后，对终端访问流量进行限速控制，用户访问应用时若流量受限有相应提示。 |
| 5. 智能连接：零信任客户端身份认证登录后支持身份驻留，提升用户访问体验性。平台支持根据身份区分不同接入点 / 接入服务，具备多网关按需接入能力（如设置多个接入点，分别负责不同人群接入，行内、外包人员登录后根据身份自动选择接入点）。 |
| 访问控制 | 1. 应用 ACL 控制：支持仅允许 IP 白名单内的主体访问指定的应用及资源，到期自动回收访问权限。支持基于环境属性（域、位置、时间、IP、信任等级）、客体属性（应用、应用菜单、应用安全标签、菜单安全标签）、操作属性（按钮）等信息的访问控制（如配置允许访问应用资源的 IP 白名单，选择资源认证级别和授权组，对不同用户进行应用和资源授权，用户登录后根据授权访问应用和资源，管理端可查看资源文件下载、浏览信息）。 |
| 2. 动态访问控制：支持提供应用 / 应用资源的动态访问控制能力，支持灵活组合规则得到不同的风险级别（如定义共有设备访问、非可信 IP 访问等规则及风险分值），执行相应的风险处置方式（高风险退出登录、中高风险禁止访问、中低风险短信增强认证、低风险安全示警），可查看风险触发的日志信息（请求时间、用户账号、应用资源、策略名称、风险分值、处置方式、风险明细）。 |
| 3. 应用可信渠道访问：支持针对 http、https 访问协议的应用进行深度报文解析，通过可信浏览器、IM、终端沙箱等渠道进行选择访问（如应用发布时设置可信访问方式，用户通过不同方式访问应用有不同结果）。支持同一应用发布到不同接入点 / 接入服务（如内网网关 / 外网关），满足不同业务场景的安全访问要求（如外网访问应用添加水印，内网访问不添加，用户在内网和外网访问应用时页面显示不同且网关节点不同）。 |
| 4. TCP/UDP 访问控制：支持 TCP、UDP 协议的应用接入（如配置 CS 应用添加 TCP 协议应用，用户通过 Xshell 访问；配置 CS 应用添加 UDP 协议应用，用户设置代理后使用腾讯会议正常通讯）。 |
| 5. 应用资源管理：支持应用概览统计能力（包括应用总数、WEB 应用数、隧道应用数等信息），提升管理员的运维能力。支持 WEB 应用 (7 层）、隧道应用 (3、4 层 TCP/UDP 应用) 的代理和发布，支持虚拟服务发布（实现应用只提供安全访问通道，而不做控制的场景）。支持 WEB 应用数据传递（可通过 URL、Header、Cookie 自定参数传递，满足应用对特定参数的需要，实现对现网应用无需修改即可正常访问），支持 WEB 应用访问透传控制（按照规则对特定 URL 不进行权限检查放过，满足对一些公共可访问的特定 URL 进行例外放行的需要）。 |
| 网络安全 | 1. 网络隐身：支持提供隐藏自身服务端口的能力，未登录和登录零信任客户端时，使用端口扫描工具扫描零信任服务 IP 及 TCP、UDP 端口，服务端均未获取到报文信息，端口扫描工具未扫描到零信任服务端开放任何端口。 |
| 2. 隧道加密：支持提供隧道内传输数据加密，加密方式支持国密算法，具备隧道断线重连的能力。登录零信任客户端访问测试应用时，抓取隧道流量显示为密文，断开网络后重新连接，客户端有隧道重连提示。 |
| 3. 网络隔离：支持提供内外网隔离的能力，开启内外区域隔离策略后，登录零信任客户端无法访问互联网地址，关闭该策略后可正常访问。 |
| 安全防护 | 1. HTTP 转 HTTPS 协议：支持 HTTP 转 HTTPS 协议的应用接入（如添加 HTTP 协议应用域名证书，配置接入应用的访问协议为 HTTPS 并关联证书，用户通过 HTTPS 访问应用可正常登录系统）。 |
| 2. 熔断流量安全保护：执行安全防护策略，保障流量安全。可新增熔断安全防护策略（设置触发保护时间、触发条件、最小请求数、超时时间、失败率阈值等），应用发布时开启熔断防护并选择相应策略，当用户访问应用满足触发条件时，跳转熔断保护页面并记录安全防护日志，熔断保护解除后可成功访问应用。 |
| 3. 风险 IP 封禁保护：智能化 IP 封禁，基于攻击防御信息自动将风险 IP 进行自动阻断。设置封禁策略（统计时间窗、累计防护次数、统计类别、封禁策略、封禁时间、是否禁止境外 IP 访问等），应用配置相应防护策略（如应用 A 配置 WAF 策略、应用 B 配置 CC 防护策略），当用户访问触发相关防护策略时，该用户网络 IP 被封禁，封禁期间无法访问任何受保护应用，封禁时间结束后才可访问。 |
| 4. Session 安全保护：防止攻击者盗用凭证登录系统。将目标应用接入零信任后，用户正常登录提取 Session，攻击者使用该 Session 在其它电脑上访问目标应用时，返回零信任平台阻断页面，可查看到攻击 IP、相应的漏洞 Payload 等阻断日志信息。 |
| 5. 网关 Bypass 功能：当网关遇到问题时，通过 bypass 功能优先保证业务正常运行。启用应用 bypass 功能后，访问应用不再会经过网关的拦截，直接跳转到应用本身页面。 |
| 安全合规审计 | 1. 统计报表：支持提供统计报表能力，通过管理平台查看统计大盘，数据至少包括用户总数、启用用户数、禁用用户数、当前在线用户数等用户信息；终端总数、启用终端数、禁用终端数等终端信息；应用总数、WEB 应用数、隧道应用数、访问应用分布等应用信息。 |
| 2. 日志审计：支持提供日志审计及日志推送能力，可查看用户登录日志、应用访问日志、管理员日志等（包括时间、用户名、登录 IP、操作信息等）。支持配置 syslog 日志推送，可自定义配置发送告警日志或系统日志等，支持发送到多个 syslog 地址，syslog 支持 tcp 和 udp 两种格式。 |
| 数据安全 | 1. 截屏 / 录屏安全防护：对受保护的应用开启 “截屏 / 录屏” 保护策略，支持截屏 / 录屏文件上传审计、截屏 / 录屏文件加密保护、截屏 / 录屏操作告警策略、禁止对此应用截屏或录屏策略（如开启策略后，截屏 / 录屏文件自动上传至服务端，本地无法打开，操作时有告警提示，禁止截屏 / 录屏时有安全提示）。 |
| 2. 数据隔离保护：支持提供数据隔离、应用管控、禁止复制、禁止粘贴、禁止截屏、禁止打印等能力。可指定应用打开渠道，设置复制粘贴保护策略；对内部分发的应用开启 “应用文件隔离”“ |

附件二：项目人员名单及人员应急退出机制

**一、项目人员名单**

项目经理：

技术骨干：

项目组成员：

**二、人员应急退出机制**

在项目实施过程中，若项目经理、技术骨干、项目组成员因工作调动、辞职等原因要离开项目组，乙方应提前一个月向甲方提出申请，经甲方同意可以更换，乙方应委派本附件约定的备用项目经理、备用技术骨干替代，涉及人员变动引起的风险、责任由乙方承担，且乙方不能因此而中断对甲方的服务，并及时启用备用人员，确保项目实施的连续性，离开人员需与备用人员办理好工作交接手续。

备用项目经理：

备用技术骨干：

附件三：验收标准及流程

**一、验收标准**

1. 验收系统须满足试运行期内项目产品运行稳定、无遗留问题。
2. 项目知识及文档已全部完成转移。

3、验收交付物包括：

《项目需求分析说明书》、《概要设计说明书》、《详细设计说明书》、《数据库设计说明书》、《系统安装部署手册》、《系统运行维护手册》、《用户操作手册》、《试运行报告》、《验收报告》、《数据迁移方案》、《系统测试计划》、《系统测试报告》、《性能测试报告》、《安全测试报告》。

**二、验收流程**

乙方负责的部分上线三个月后，由甲方按照合同进行验收，验收通过，在验收表上签字或盖章；若验收过程中发现与合同有偏差或系统问题，则由甲方提交验收问题报告给乙方，乙方按验收问题报告进行相应改进。改进完成后，重新验收。

附件四：维护服务条款

乙方业务代表作为技术服务的第一联系人，项目经理作为该项目的技术服务第二联系人，随时接受客户的电话服务支持，并申请调配相关资源为客户提供及时服务。

1. 系统正式验收通过，上线后提供三个月免费人员现场驻场维护，正式验收合格次日至次年并延期至6月30日或12月31日中较近日期（即维保延期最长不超过半年）提供支持和服务。
2. 维护期内，提供平台升级及优化服务。
3. 系统上线后，提供二次系统和产品的培训，时间为每次1天。在维护期内，也可以根据用户需求，随时到客户现场进行系统和产品的培训。
4. 维护期内，每季度派工程师现场巡检一次，并在巡检后提交巡检报告，针对巡检中发现的问题立即组织整改。

支持方式和手段

1. 热线电话

针对具体业务过程中产生的各种技术咨询，开设专线，提供7\*24小时的技术服务支持。

1. E-mail

客户建议、意见及技术支持同样可以通过XXXXX公司（乙方）提供的服务支持电子信箱获得响应，我们将做出详细、全面的服务解答，在半天内给予E-mail回复。

1. 远程登录

对客户所遇到技术问题可以在客户条件许可的情况下进行远程访问排除故障，以方便客户能够及时解决疑难杂症。

1. 现场支持

对于重大故障或者无法通过远程登录排除的故障，将安排工程师前往现场进行处理，使客户在最短的时间内解决故障，减少故障历时，从而最大限度地减少客户损失，保证在2小时内到现场。

1. 运行日志定期检查

最好的服务方式是提前发现问题，将问题解决于发生前，在乙方实施的系统中，提供了相关的运行日志，通过和客户的协商，通过客户定期提供的运行日志，可实现定期的日志检查，可以提前发现系统的运行问题，以起到防患于未然的效果。

1. 故障处理流程

通过现象定位错误原因，编写处理说明书（包含处理完成时间）。

附件五：服务水平协议（SLA）

**1. 目标**

本服务水平协议（SLA）的目标是为了清晰地定义由XXXXXXXXXXXX公司（乙方）在本项目中为重庆三峡银行（甲方）提供的服务水平，本SLA主要：

* 明确甲方对外包乙方所提供服务水平的期望
* 规范和加强甲方对乙方所提供服务水平的控制

双方将针对本项目制定明确的职责分工表用来确定计划和管理服务水平协议的角色和职责。

**2. 协议期限**

根据双方达成的一致要求，本协议的有效期从本项目实施之日起到合同正文6.1承诺的维护期结束。

**3. 双方职责**

**3.1乙方**

除本协议描述的服务水平衡量和目标外，乙方还应：

* 尽快向甲方管理层汇报发现的问题；
* 任何可能影响SLA中规定服务的服务能力的事件，乙方应尽早向甲方提供预警信息，以及可能的影响和处置措施。事件包括：
* 组织架构变更
* 技术变更
* 职能变更
* 其他可能影响对甲方服务的突发事件
* 协助甲方及时解决生产事件。当问题产生时，应尽快采取适当的措施识别并修复问题。

**3.2甲方**

* 甲方将尽快将问题汇报给乙方管理层；
* 提供任何可能影响乙方向甲方提供SLA中规定服务的服务能力的事件信息，包括：
* 组织架构变更
* 技术变更
* 职能变更

**4. 服务内容**

|  |  |  |
| --- | --- | --- |
| 4.1技术管理 | | |
| 4.1.1 | 项目执行控制 | 管理目标、沟通和范围 |
| 4.1.2 | 系统部署 | 在甲方所提供的技术环境内配置和部署系统接入所需的资源 |
| 4.1.3 | 管理系统 | 管理运行过程中的各个环节和环境（如测试、培训、维护等） |
| 4.2系统处理 | | |
| 4.2.1 | 备份 | 提供数据容量规划咨询，设计系统的备份策略，完成其有效性验证 |
| 4.2.2 | 恢复 | 设计系统的恢复策略，完成其有效性验证 |
| 4.3软件开发及测试 | | |
| 4.3.1 | 软件管理 | 负责管理和设计应用软件，配合进行软件过程开发管理 |
| 4.3.2 | 系统接口开发 | 设计和开发系统内部各模块的接口以及与外部系统进行数据交互的接口 |
| 4.3.3 | 代码开发和测试 | 编写代码并且完成开发自测与系统测试 |
| 4.3.4 | 知识转移 | 负责现场培训 |
| 4.4 支持和维护 | | |
| 4.4.1 | 变更管理 | 根据变更需求在甲方的技术环境内设计并且执行所有平台和应用软件变更程序 |
| 4.4.2 | 系统监控 | 提供对系统监控的支持，包括专有硬件设备（如有）、应用系统进程、日志、连接等 |
| 4.4.3 | 发布管理 | 制定测试环境发布方案，协助将具体的目标系统从测试环境移植到生产的上线方案 |
| 4.4.4 | 安全管理 | 配合甲方完成上线前的漏洞扫描、渗透测试等安全评估工作，根据甲方要求完成发现漏洞的整改工作 |
| 4.5 后续支持 | | |
| 4.5.1 | 版本安装、更新和升级 | 提供系统版本安装和升级支持，包括响应甲方对生产、测试、开发、培训环境的安装和升级要求；提供硬件更换服务 |
| 4.5.2 | 安全漏洞整改 | 针对系统运行过程中发现的安全漏洞，根据甲方要求完成整改工作 |
| 4.5.3 | 服务台支持 | 提供7×24小时的技术支持服务 |
| 4.5.4 | 巡检服务 | 提供系统运行状况报告 |
| 4.5.5 | 现场问题解决 | 提供重大问题现场解决，提供系统性能、容量、问题报告 |
| 4.5.6 | 响应要求 | 要求按服务水平和指标及时响应：  一级响应：系统崩溃,不能使用或效能严重削弱, 系统的某个主要功能不能正常工作，对业务的正常运行造成重大影响。响应时间15分钟，2小时到达现场，4小时内排除问题或给出备份解决方案，故障排除后三天内提交分析报告；  二级响应：系统的运行性能严重下降，或性能明显下降，对业务运作产生明显影响。响应时间1小时内，必要时4小时到达，8小时内排除问题；  三级响应：系统的运作性能受损，但业务仍可正常运行，响应时间12小时内，必要时24小时到达，1周内排除问题；  四级响应：对系统安装或配置方面需要咨询或支援，很显然对业务运作几乎无影响，或根本没有影响。响应时间24小时内，必要时48小时到达，2周内排除问题。 |

**5. 问题管理流程**

**5.1问题处理流程**

1. 甲方或乙方均可以首先提出对问题解决方案有不同意见的看法；
2. 甲方管理层和乙方管理层将决定问题是否需要提升到更高的管理层；
3. 及时召开相关的会议讨论和解决问题，问题的相关文档应提前一天发送到与会者；
4. 如有必要，甲方和乙方管理层在永久性解决方案出台之前可以先共同达成一套临时性的解决方案。乙方可以在会后与各利益相关方沟通并达成永久性的解决方案；
5. 如果问题最终仍没解决，甲方和乙方双方可以申请仲裁来达成最终的一致方案。

**5.2问题升级流程**

* 甲方或者乙方都有可能首先提出该流程；
* 首先提出的一方应及时通知对方问题升级流程已经启动；
* 问题升级到的管理层应当事先定义在联络人表中；
* 问题升级的层次在甲方和乙方之间应当保持一致，直至解决该问题。

**5.3联络表**

|  |  |  |
| --- | --- | --- |
| **乙方** | **职务** | **电话** |
|  | 商务代表 |  |
|  | 项目经理 |  |
|  | 项目总监 |  |
|  | 总经理 |  |

**6. 汇报内容及流程**

乙方应当在每星期五向甲方提交工作周报，包括项目情况跟踪及问题报告等，附带的性能报告（如有）也将递交给甲方项目经理。如发生突发事件，乙方也应第一时间向甲方项目经理报告。

**7. 服务水平和指标**

* 甲方将定期对乙方进行考评，乙方提供的服务必须满足以下服务水平和指标要求，否则按违约金标准收取相应金额违约金。合计金额按主合同违约责任约定限定，以人民币计算，由甲方直接扣除合同款项。乙方签订本合同即认可其派驻的项目经理被赋予项目管理的签字权，其签字内容承担相应的违约责任。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **评价**  **维度** | **评价**  **指标** | **指标定义** | **评分/价标准** | **违约金标准** | **评价**  **结果** | **评价**  **得分** |
| 1 | 服务质量 | 交付成果质量 | 用于记录乙方所提交的项目交付成果与甲方要求的项目交付成果的契合度或交付成果质量与合同所约定要求的项目交付成果质量的满足程度 | **优秀：**5分，指乙方能够主动快速与甲方进行有效的沟通，交付成果高度契合需求，完全满足并超出合同约定的预期目标，给甲方带来显著的附加价值；  **良好：**4分，指乙方能够快速响应需求，交付成果达到合同约定的预期目标，基本契合需求，满足合同约定的预期目标；  **合格：**3分，指乙方能够按要求响应需求，交付成果基本满足需求，但是总体可满足合同约定的预期目标；  **较差/差：**0分，指乙方未能够按要求响应需求，或交付成果与需求契合度差距较大，无法达到合同约定的预期目标。 | 交付成果每缺少一项扣除乙方金额人民币2000元；每有一项交付成果质量不合格扣除乙方金额人民币2000元。 |  |  |
| 2 | 成果交付延期情况 | 用于记录因乙方原因导致项目交付成果时间与合同规定时间之间的差距 | 实际交付成果日期与合同约定交付日期之差**【得分上限5分】**  **无延期：**指未出现延期，该项指标满分；  **0＜延期≤3个月：**扣2分，指出现延期3个月（含）以内；  **3＜延期≤6个月：**扣3分，指出现延期大于3个月且小于等于6个月；  **延期6个月以上：**扣5分，指出现延期6个月以上。 | 若延期超过1个月，每延期增加一天扣除合同总金额的0.1%（注：最多扣除不超过合同总金额的10%） |  |  |
| 3 | 产品缺陷密度 | 用于记录统计周期内单位功能（案例）点发现的缺陷数量 | 产品缺陷密度=统计周期内发现的该系统有效缺陷数/统计周期内该系统功能点总数（案例数）  **10分【0-5%】**  **5分【5%-20%】**  **0分【超过20%】** | 产品缺陷密度超过20%，缺陷密度每增加1%扣除合同总金额的0.1%。 |  |  |
| 4 | 缺陷解决率 | 用于记录统计周期内测试发现的缺陷中已解决缺陷的比例 | 缺陷解决率=统计周期内测试发现的有效缺陷中已解决的数量/统计周期内测试发现的有效缺陷总数量  **10分【98%-100%】**  **5分【95%-97%】**  **0分【低于95%】** | 若缺陷解决率低于95%，缺陷解决率每低1%扣除合同总金额的0.1%。 |  |  |
| 5 | 协议履行 | 重大事项报告 | 用于记录乙方应对自身的财务、内控及安全管理进行持续监控，将自身因破产、兼并、关键人员流失、投入不足和管理不善等引发的财务状况恶化及内部管理混乱等情况告知甲方的评价 | **优秀：**5分，指无重大事项或当发生重大事项时，能够于24小时内告知甲方；  **良好：**4分，指当发生重大事项时，能够于一周内告知甲方；  **合格：**3分，指当发生重大事项时，能够于一月内告知甲方；  **较差/差**：0分，指当发生重大事项时，未告知甲方。 | 评价为较差/差时，甲方根据实际情况有权终止合同，并要求乙方赔偿实际损失。 |  |  |
| 6 | 重大事件及质量缺陷 | 用于记录乙方在服务期内出现以下重大事件及质量缺陷次数：  a.应用软件出现III级（含）以上的运营中断事件；  b.因乙方原因（含乙方合作的第三方）导致甲方发生网络安全事件；  c.应用软件出现严重缺陷和致命缺陷。 | **【得分上限10分】**  **0次：**指未出现重大事件及质量缺陷，该项指标满分；  **1次及以上：**0分，指出现1次及以上任意一项重大事件或质量缺陷。 | 每出现一次重大事件或质量缺陷，扣除乙方合同总金额不低于5%（不低于2万元），并要求乙方赔偿实际损失。 |  |  |
| 7 | 信息安全管理 | 用于记录乙方在服务期内网络和信息安全服务的管理能力，针对发现的安全漏洞及安全缺陷（包括源代码、第三方SDK或第三方小程序、第三方软件产品及开源组件等），须按甲方要求完成整改 | 互联网或电子银行类系统：  1.安全漏洞及安全缺陷整改及时率=100%  2.安全漏洞及安全缺陷整改通过率=100%  非互联网或电子银行类系统：  1.中高危安全漏洞及安全缺陷整改及时率=100%  2.中高危安全漏洞及安全缺陷整改通过率=100%  **优秀：**5分，指未出现安全漏洞及安全缺陷，该项指标满分；  **合格：**3分，指出现安全漏洞或安全缺陷，但整改及时率、通过率均为100%；  **较差/差：**0分，指出现安全漏洞及安全缺陷，但整改及时率或通过率未达到100%。 | 若出现的安全漏洞或安全缺陷被上级或监管单位通报的，扣除乙方金额人民币不低于2万元；  若评价为较差/差时，扣除乙方金额人民币不低于2万元，并要求乙方赔偿实际损失。 |  |  |
| 8 | 外包安全行为 | 用于记录乙方在服务期内出现危害甲方生产运行安全、数据安全的外包安全行为风险（包括但不限于泄露甲方内部信息、破坏测试环境数据，在生产运营系统上违反规定进行操作或在实施过程中留下信息系统后门等行为） | **【得分上限10分】**  **0次：**指乙方服务未出现外包安全行为风险，该项指标满分；  **1次及以上：**指乙方出现1次及以上外包安全行为风险（每次扣5分，最高扣除10分）。 | 每发生一次外包安全行为风险，扣除乙方金额人民币不低于1000元，并要求乙方赔偿实际损失。 |  |  |
| 9 | 响应与解决及时性 | 用于记录乙方或服务项目对甲方的响应与解决的及时性 | **优秀：**5分，指乙方或服务项目能够迅速响应需求，主动快速与甲方进行有效的沟通，第一时间从专业角度给出解决方案并解决问题；  **良好：**4分，指乙方或服务项目能够按要求响应需求，及时与甲方进行有效的沟通，快速给出处理方案并解决问题；  **合格：**3分，指乙方或服务项目能够基本按要求响应需求，保持与甲方的沟通，按时解决问题；  **较差/差：**0分，指乙方或服务项目未及时响应需求，或响应需求后无法及时解决问题。 | 评价为较差/差，即乙方或服务项目未及时响应需求，或响应需求后无法及时解决问题，扣除乙方金额人民币不低于1000元。 |  |  |
| 10 | 需求排期率 | 用于记录统计周期内对甲方需求进行投产计划安排的比例 | 需求排期率=已排期需求数/总需求数  注：已排期需求数指统计周期内已经纳入投产计划的需求个数。总需求数指统计周期内由甲方提出到达服务商项目组的需求数。  **5分【98%-100%】**  **3分【95%-97%】**  **0分【低于95%】** |  |  |  |
| 11 | 需求完成率 | 用于记录统计周期内甲方需求完成投产的比例 | 需求完成率=流程完结需求数/总需求数  注：流程完结需求数指统计周期内已完成投产的需求个数；总需求数指统计周期内由甲方提出到达服务商项目组的需求个数。  **5分【98%-100%】**  **3分【95%-97%】**  **0分【低于95%】** |  |  |  |
| 12 | 人员行为规范性 | 用于记录外包场地日常管理或检查过程中发现外包人员行为违规（包括但不限于办公纪律、造成办公环境物理安全隐患等）的次数 | **【得分上限10分】**  **0次：**指未出现外包人员行为违规，该项指标满分；  **1次及以上：**指检查发现外包人员行为违规1次及以上（每人次扣5分，最高扣除10分） | 每出现一次人员行为违规，扣除乙方金额人民币不低于500元。 |  |  |
| 13 | 人员变动率 | 用于记录统计周期内乙方未经甲方同意更换外包人员数量占乙方驻场外包人员总数量的比率 | 人员变动率=乙方未经甲方同意更换外包人员数量/乙方驻场外包人员总数量  **10分【0-20%】**  **5分【20%-40%】**  **0分【超过40%】** | 技术骨干或项目经理未经甲方同意变动，扣除乙方金额人民币不低于3万元；其余人员变动率超过40%，扣除不低于合同总金额的1%。 |  |  |
| 14 | 人员满意度评价 | 甲方对乙方外包人员表现的满意度评价 | **优秀：**5分，指工作效率高，态度积极主动，保质保量完成工作任务，对团队有突出贡献，日常行为能起到模范带头作用的；  **良好：**4分，指工作效率较高，态度比较主动，较好完成工作任务，对团队有一定贡献，日常行为表现较好的；  **合格：**3分，指工作效率一般，态度合格，能够按时完成工作任务的；  **较差/差：**0分，指工作效率低下，态度懈怠散漫，不能按时完成工作任务的。 | 评价为较差/差时，甲方有权要求乙方更换人员并赔偿实际损失。 |  |  |
| 综合得分： | | | | | | |  |
| 综合评价：  （注：请开展综合评价，不满足服务要求的，需详细阐述不满足的内容及扣除合同违约金，填写完成后删除此括号内容）  评价人： | | | | | | | |

注：综合评价等级划分优秀、良好、合格、差

优秀：评价得分达90分以上；

良好：评价得分达75-90分；

合格：评价得分达60-75分；

附件六：服务连续性预案

**一、目的**

为保证甲方项目实施的及时性、连续性和稳定性，避免由于外包服务中断而引起项目中断、项目目标无法达成，故拟定本外包服务中断场景时的应急方案，作为突发外包服务中断事件时的服务恢复依据。

**二、应急组织架构及职责**

**（一）决策层**

|  |  |  |  |
| --- | --- | --- | --- |
| 角色 | 姓名 | 联系方式 | 职责 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**（二）危机处理层**

|  |  |  |  |
| --- | --- | --- | --- |
| 角色 | 姓名 | 联系方式 | 职责 |
|  |  |  |  |
|  |  |  |  |

**（三）具体业务层**

|  |  |  |  |
| --- | --- | --- | --- |
| 角色 | 姓名 | 联系方式 | 职责 |
|  |  |  |  |
|  |  |  |  |

**（四）应急领导小组职责**

1.启动应急预案

对突发事件进行处置，确保业务的持续性；对项目突发事件业务影响情况进行分析和评估；收集分析项目突发事件应急处置过程中的业务信息、数据、日志；向甲方报告应急处置进展情况和事态发展情况。

2.应急事件处理

负责详细记录并分析应急事件，在项目组人员及其他资源的协助下，提出应急事件解决方案，并负责向甲方解释应急事件及方案；当解决方案通过甲方审核后，由危机处理层负责方案的实施，并在实施结束后，提交“应急事件处理报告”。

3.业务持续性计划及应急预案优化

负责每个月针对当月及以往产生的应急事件实施报告，对现有的业务持续性计划及应急预案进行评估，当发现存在风险时，需要进行相应的优化；优化后的业务持续性计划及应急预案必须提交甲方审核，并按照审核通过后的新计划进行实施。

**三、应急场景**

**（一）单个核心成员或某个角色无法提供正常服务**

1.影响程度：外包服务部分中断

2.规避措施：

1）乙方在2小时内协调重庆本地高于该成员资历水平的的员工来厂商现场进行顶替，直到合适的补充人员入场能够接替该成员的工作为止，否则按照SLA第6调更换人员的相关条款进行罚款。

2）乙方服务团队在合同有效期内，建立人才储备机制和培训机制，同时由A角和B角对项目进行支持工作。因乙方原因造成甲方损失的，乙方按照SLA进行赔偿。

**（二）乙方服务团队无法提供正常服务，但乙方仍具备履约能力**

1.影响程度：外包服务完全中断

2.规避措施：

1）乙方服务团队需按时按照甲方流程及制度规范提交项目各类文档；

2）乙方服务团队需制定合理的培训计划和培训内容，加强知识转移；

3）如遇类似事件乙方提前10个工作日书面通知甲方项目经理；

4）乙方负责提前协调备用团队，并协调相应角色做好交接工作，协调方案经过甲方认可后，在10个工作日内将补充团队派驻入场，保障工作连续开展。因乙方原因造成甲方损失的，乙方在双方协商后做出赔偿。

**（三）乙方服务团队无法提供正常服务且乙方不具备恢复服务能力或意愿**

1.影响程度：外包服务完全中断

2.规避措施：

1）如遇类似事件乙方提前15个工作日书面通知甲方项目经理；

2）乙方保证提前沟通协调人力资源，于10个工作日内提交所有阶段性项目文档，并完成甲方认可的所有工作交接和知识转移，包括不限于对替代供应商进行培训；

3）允许推荐项目成员到与甲方合作良好的其他供应商任职或由甲方直接聘用。因乙方原因造成甲方损失的，乙方在双方协商后做出赔偿。

**（四）乙方因资质变更、被收购、兼并或破产等原因致使其无法继续提供服务**

1.影响程度：外包服务完全中断

2.规避措施：

1）如遇类似事件乙方提前20个工作日通知甲方项目经理；

2）根据开发合同约定提前与甲方进行沟通协商，做好代码、文档、服务等交接工作，减少对甲方的影响；

3）乙方保证提前沟通协调人力资源，于15个工作日内提交所有阶段性项目文档，并完成甲方认可的所有工作交接和知识转移，包括不限于对替代供应商进行培训。因乙方原因造成甲方损失的，乙方在双方协商后做出赔偿；

4）允许推荐项目成员到与甲方合作良好的其他供应商任职或由甲方直接聘用。

**（五）乙方因不可抗力导致其主动退出（国家相关法律法规调整、遭受大规模自然灾害等）**

1.影响程度：外包服务完全中断

2.规避措施：

1）如遇类似事件乙方应立即通知甲方项目经理。

2）乙方与甲方及时进行协商，得出一致性解决方案，于15个工作日内提交所有阶段性项目文档，并完成甲方认可的所有工作交接和知识转移，降低突发事件的影响；

3）允许推荐项目成员到与甲方合作良好的其他供应商任职或由甲方直接聘用。因乙方原因造成甲方损失的，乙方在双方协商后做出赔偿。

**四、应急处理阶段**

**（一）项目实施过程中应急服务**

乙方应急小组进行突发事件业务影响情况的分析和评估，应急领导小组根据事态发展情况提出应急事件处理方案，并进行应急任务的分配和人员及应急资源的调度工作，保证在最短时间内完成项目现场的应急行动，并向甲方及时反馈后续事件的处理。

在应急事件处理完毕后，由乙方应急小组对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，总结经验教训，完善应急处理预案，整改项目服务过程中存在的隐患问题。

**（二）系统上线后应急服务**

甲方可以通过拨打乙方服务团队技术支持热线电话或发送邮件的方式，向乙方专业技术人员咨询应用系统的有关问题、报告故障信息、获得排除系统运行故障的方法或指导。乙方开发人员及联系方式如下：

姓名: 手机号码：邮箱：

姓名: 手机号码：邮箱：

# 第六章 响应文件格式

重庆三峡银行

零信任安全平台项目

响 应 文 件

响应人： （盖单位公章）

年 月 日

**目 录**

一、响应函

二、报价一览表

三、资格性文件

（一）响应人基本情况介绍，资质证明等

（二）法定代表人/分支机构负责人身份证明及授权委托书

（三）书面声明

（四）中国执行信息公开网截图

（五）项目案例和业绩证明文件复印件

（六）认证证明材料

（七）其他（如有）

四、响应性文件

（一）响应承诺函

（二）服务水平协议（SLA）

（三）社保材料及相关证明材料

（四）服务连续性预案

（五）项目实施方案

（六）售后服务和培训方案

（七）其他（如有）

五、商务技术文件（如有）

六、其他（如有）

一、响应函

重庆三峡银行股份有限公司：

我方收到 （项目名称）询比文件，经详细研究，决定参加该询比项目并响应。

1、愿意按照询比文件中的一切要求，以响应文件中的内容和报价承担和完成本项目。

2、我方现提交的响应文件为：响应文件正本一份，副本一份，电子文件一份。

3、如果我方响应文件被接受，我方将履行询比文件中规定的各项要求，按相关法律法规和合同约定条款承担我方的责任。

4、我方愿意提供询比文件中要求的所有资料，并对其真实性负责。

5、我方理解最低价格不是成交的唯一条件。

6、响应有效期为响应截止日期后90天内。

7、若我方成交，我方开具税率为 %的增值税专用发票；

响应人（公章）：

响应人联系人：

响应人联系人联系电话：

年 月 日

二、报价一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 响应人全称 |  | | |
| 项目名称 |  | | |
| 响应总报价（含税） | 小写： 人民币  大写： 人民币 | | |
| 响应总报价（不含税） | 小写： 人民币  大写： 人民币 | | |
| 免费维保期 |  | 免费维保期后的维保费率 |  |
| 开具发票类型 | 税率为 %的增值税专用发票 | | |
| 备注： | | | |

注：上述税率为推荐税率，因国家政策产生的特殊情况除外，若有税收优惠请附相关凭证。若遇国家税率调整，则保持不含税价不变，重新计算含税价格。

响应人：

（公章）

年 月 日

有关说明：

报价一览表在开标大会上当众宣读，务必填写清楚，准确无误。表格可扩展。

本次报价包含上述维护期的，采购人不再另行支付该维护期内维护费用。

三、资格性文件

（一）响应人基本情况介绍，资质证明等

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 响应人名称 |  | | | | | | | |
| 注册地址 |  | | | | 邮政编码 |  | | |
| 联系方式 | 联系人 |  | | | 电话 |  | | |
| 传真 |  | | | 网址 |  | | |
| 组织结构 |  | | | | | | | |
| 法定代表人/分支机构负责人 | 姓名 |  | 技术职称 | |  | | 电话 |  |
| 技术负责人 | 姓名 |  | 技术职称 | |  | | 电话 |  |
| 成立时间 |  | | 员工总人数： | | | | | |
| 企业资质等级 |  | | 其中 | 项目经理 | | |  | |
| 营业执照号 |  | | 高级职称人员 | | |  | |
| 注册资金 |  | | 中级职称人员 | | |  | |
| 开户银行 |  | | 初级职称人员 | | |  | |
| 账号 |  | | 技工 | | |  | |
| 经营范围 |  | | | | | | | |
| 备注 |  | | | | | | | |

注：附营业执照（副本）、总公司授权委托书、资质证明复印件等。

（二）法定代表人/分支机构负责人身份证明及授权委托书

法定代表人/分支机构负责人身份证明书

项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

致： 重庆三峡银行股份有限公司 ：

（响应人法定代表人/分支机构负责人姓名）在 （响应人名称）任 （职务名称）职务，是（响应人名称） 的法定代表人/分支机构负责人。

特此证明。

响应人：

（响应人公章）

年 月 日

（附：法定代表人/分支机构负责人身份证正反面复印件）

授权委托书（如有）

（适用于有委托代理人的情况时采用）

项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

致：重庆三峡银行股份有限公司：

（响应人法定代表人/分支机构负责人名称）是 （响应人名称）的法定代表人（分支机构负责人），特授权 （委托代理人姓名及身份证代码）代表我单位全权办理上述项目的响应、谈判、签约等具体工作，并签署全部有关文件、协议及合同。

我单位对委托代理人的签字负全部责任。

在撤销授权的书面通知以前，本授权书一直有效。委托代理人在授权书有效期内签署的所有文件不因授权的撤销而失效。

|  |  |
| --- | --- |
| 委托代理人 | 响应人法定代表人/分支机构负责人名称： |
| （签字或盖章） | （签字或盖章） |

（附：委托代理人身份证正反面复印件）

响应人：

（响应人公章）

年 月 日

注：若为法定代表人（分支机构负责人）办理并签署响应文件的，不提供此文件。

（三）书面声明

项目名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

致：重庆三峡银行股份有限公司：

（响应人名称）郑重声明，我公司为产品原厂商，具备对产品二次开发及维护能力，近3年财务状况稳定，具有良好的商业信誉和健全的财务会计制度，具有履行合同所必需的设备和专业技术能力，具有依法缴纳税收和社会保障金的良好记录，在合同签订前后随时愿意提供相关证明材料；我公司还同时声明参加本项目询比活动前三年内无重大违法活动记录，符合法律法规规定的响应人资格条件；我公司本次如若成交，成交后不会对项目进行转包。我方对以上声明负全部法律责任。

特此声明。

（响应人公章）

年 月 日

（四）中国执行信息公开网截图

1.法人在中国执行信息公开网的查询截图并加盖单位鲜章

2.法定代表人在中国执行信息公开网的查询截图并加盖单位鲜章

（五）项目案例和业绩证明文件复印件

1、合同关键页（合同关键页包含：甲乙双方名称、双方印章、项目名称、合同签订时间、服务范围。）

2、项目简介（格式自拟）

3、合同对应的发票之一（网上税务系统查询（https://inv-veri.chinatax.gov.cn/）该发票的截图，发票开具日期须晚于合同签订日期、发票购买方须与合同买方一致、发票销售方须与合同卖方（响应人）一致）。】

（六）认证证明材料

（七）其他（如有）

四、响应性文件

（一）响应承诺函

根据第三章“项目要求”内容，做出整体承诺，格式自理。

根据第三章第9条相关内容进行阐述并作出相应承诺。

（二）服务水平协议（SLA）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 评价  维度 | 评价  指标 | 指标定义 | 评分/价标准 | 违约金标准 |
| 1 | 服务质量 | 交付成果质量 | 用于记录乙方所提交的项目交付成果与甲方要求的项目交付成果的契合度或交付成果质量与合同所约定要求的项目交付成果质量的满足程度 | 优秀：5分，指乙方能够主动快速与甲方进行有效的沟通，交付成果高度契合需求，完全满足并超出合同约定的预期目标，给甲方带来显著的附加价值；  良好：4分，指乙方能够快速响应需求，交付成果达到合同约定的预期目标，基本契合需求，满足合同约定的预期目标；  合格：3分，指乙方能够按要求响应需求，交付成果基本满足需求，但是总体可满足合同约定的预期目标；  较差/差：0分，指乙方未能够按要求响应需求，或交付成果与需求契合度差距较大，无法达到合同约定的预期目标。 | 交付成果每缺少一项扣除乙方金额人民币2000元；每有一项交付成果质量不合格扣除乙方金额人民币2000元。 |
| 2 | 成果交付延期情况 | 用于记录因乙方原因导致项目交付成果时间与合同规定时间之间的差距 | 实际交付成果日期与合同约定交付日期之差【得分上限5分】  无延期：指未出现延期，该项指标满分；  0＜延期≤3个月：扣2分，指出现延期3个月（含）以内；  3＜延期≤6个月：扣3分，指出现延期大于3个月且小于等于6个月；  延期6个月以上：扣5分，指出现延期6个月以上。 | 若延期超过1个月，每延期增加一天扣除合同总金额的0.1%（注：最多扣除不超过合同总金额的10%） |
| 3 | 产品缺陷密度 | 用于记录统计周期内单位功能（案例）点发现的缺陷数量 | 产品缺陷密度=统计周期内发现的该系统有效缺陷数/统计周期内该系统功能点总数（案例数）  10分【0-5%】  5分【5%-20%】  0分【超过20%】 | 产品缺陷密度超过20%，缺陷密度每增加1%扣除合同总金额的0.1%。 |
| 4 | 缺陷解决率 | 用于记录统计周期内测试发现的缺陷中已解决缺陷的比例 | 缺陷解决率=统计周期内测试发现的有效缺陷中已解决的数量/统计周期内测试发现的有效缺陷总数量  10分【98%-100%】  5分【95%-97%】  0分【低于95%】 | 若缺陷解决率低于95%，缺陷解决率每低1%扣除合同总金额的0.1%。 |
| 5 | 协议履行 | 重大事项报告 | 用于记录乙方应对自身的财务、内控及安全管理进行持续监控，将自身因破产、兼并、关键人员流失、投入不足和管理不善等引发的财务状况恶化及内部管理混乱等情况告知甲方的评价 | 优秀：5分，指无重大事项或当发生重大事项时，能够于24小时内告知甲方；  良好：4分，指当发生重大事项时，能够于一周内告知甲方；  合格：3分，指当发生重大事项时，能够于一月内告知甲方；  较差/差：0分，指当发生重大事项时，未告知甲方。 | 评价为较差/差时，甲方根据实际情况有权终止合同，并要求乙方赔偿实际损失。 |
| 6 | 重大事件及质量缺陷 | 用于记录乙方在服务期内出现以下重大事件及质量缺陷次数：  a.应用软件出现III级（含）以上的运营中断事件；  b.因乙方原因（含乙方合作的第三方）导致甲方发生网络安全事件；  c.应用软件出现严重缺陷和致命缺陷。 | 【得分上限10分】  0次：指未出现重大事件及质量缺陷，该项指标满分；  1次及以上：0分，指出现1次及以上任意一项重大事件或质量缺陷。 | 每出现一次重大事件或质量缺陷，扣除乙方合同总金额不低于5%（不低于2万元），并要求乙方赔偿实际损失。 |
| 7 | 信息安全管理 | 用于记录乙方在服务期内网络和信息安全服务的管理能力，针对发现的安全漏洞及安全缺陷（包括源代码、第三方SDK或第三方小程序、第三方软件产品及开源组件等），须按甲方要求完成整改 | 互联网或电子银行类系统：  1.安全漏洞及安全缺陷整改及时率=100%  2.安全漏洞及安全缺陷整改通过率=100%  非互联网或电子银行类系统：  1.中高危安全漏洞及安全缺陷整改及时率=100%  2.中高危安全漏洞及安全缺陷整改通过率=100%  优秀：5分，指未出现安全漏洞及安全缺陷，该项指标满分；  合格：3分，指出现安全漏洞或安全缺陷，但整改及时率、通过率均为100%；  较差/差：0分，指出现安全漏洞及安全缺陷，但整改及时率或通过率未达到100%。 | 若出现的安全漏洞或安全缺陷被上级或监管单位通报的，扣除乙方金额人民币不低于2万元；  若评价为较差/差时，扣除乙方金额人民币不低于2万元，并要求乙方赔偿实际损失。 |
| 8 | 外包安全行为 | 用于记录乙方在服务期内出现危害甲方生产运行安全、数据安全的外包安全行为风险（包括但不限于泄露甲方内部信息、破坏测试环境数据，在生产运营系统上违反规定进行操作或在实施过程中留下信息系统后门等行为） | 【得分上限10分】  0次：指乙方服务未出现外包安全行为风险，该项指标满分；  1次及以上：指乙方出现1次及以上外包安全行为风险（每次扣5分，最高扣除10分）。 | 每发生一次外包安全行为风险，扣除乙方金额人民币不低于1000元，并要求乙方赔偿实际损失。 |
| 9 | 响应与解决及时性 | 用于记录乙方或服务项目对甲方的响应与解决的及时性 | 优秀：5分，指乙方或服务项目能够迅速响应需求，主动快速与甲方进行有效的沟通，第一时间从专业角度给出解决方案并解决问题；  良好：4分，指乙方或服务项目能够按要求响应需求，及时与甲方进行有效的沟通，快速给出处理方案并解决问题；  合格：3分，指乙方或服务项目能够基本按要求响应需求，保持与甲方的沟通，按时解决问题；  较差/差：0分，指乙方或服务项目未及时响应需求，或响应需求后无法及时解决问题。 | 评价为较差/差，即乙方或服务项目未及时响应需求，或响应需求后无法及时解决问题，扣除乙方金额人民币不低于1000元。 |
| 10 | 需求排期率 | 用于记录统计周期内对甲方需求进行投产计划安排的比例 | 需求排期率=已排期需求数/总需求数  注：已排期需求数指统计周期内已经纳入投产计划的需求个数。总需求数指统计周期内由甲方提出到达服务商项目组的需求数。  5分【98%-100%】  3分【95%-97%】  0分【低于95%】 |  |
| 11 | 需求完成率 | 用于记录统计周期内甲方需求完成投产的比例 | 需求完成率=流程完结需求数/总需求数  注：流程完结需求数指统计周期内已完成投产的需求个数；总需求数指统计周期内由甲方提出到达服务商项目组的需求个数。  5分【98%-100%】  3分【95%-97%】  0分【低于95%】 |  |
| 12 | 人员行为规范性 | 用于记录外包场地日常管理或检查过程中发现外包人员行为违规（包括但不限于办公纪律、造成办公环境物理安全隐患等）的次数 | 【得分上限10分】  0次：指未出现外包人员行为违规，该项指标满分；  1次及以上：指检查发现外包人员行为违规1次及以上（每人次扣5分，最高扣除10分） | 每出现一次人员行为违规，扣除乙方金额人民币不低于500元。 |
| 13 | 人员变动率 | 用于记录统计周期内乙方未经甲方同意更换外包人员数量占乙方驻场外包人员总数量的比率 | 人员变动率=乙方未经甲方同意更换外包人员数量/乙方驻场外包人员总数量  10分【0-20%】  5分【20%-40%】  0分【超过40%】 | 技术骨干或项目经理未经甲方同意变动，扣除乙方金额人民币不低于3万元；其余人员变动率超过40%，扣除不低于合同总金额的1%。 |
| 14 | 人员满意度评价 | 甲方对乙方外包人员表现的满意度评价 | 优秀：5分，指工作效率高，态度积极主动，保质保量完成工作任务，对团队有突出贡献，日常行为能起到模范带头作用的；  良好：4分，指工作效率较高，态度比较主动，较好完成工作任务，对团队有一定贡献，日常行为表现较好的；  合格：3分，指工作效率一般，态度合格，能够按时完成工作任务的；  较差/差：0分，指工作效率低下，态度懈怠散漫，不能按时完成工作任务的。 | 评价为较差/差时，甲方有权要求乙方更换人员并赔偿实际损失。 |

（三）社保材料及相关证明材料

（四）服务连续性预案

（应考虑供应链风险产生的影响）

（五）项目实施方案

（实施方案包括履行合同的时间计划、提交资料、人员安排等）

（六）售后服务和培训方案

（七）其他（如有）

（如第三章中要求提供的文件、方案等材料）

五、商务技术文件（如有）

（根据第四章内容提供相关材料）

六、其他（如有）