《金融科技创新应用声明书》

<table>
<tr><td rowspan="8">创新应用基本信息</td><td>创新应用编号</td><td colspan="2">91130629MA09UT5P4E-2020-0001</td></tr>
<tr><td>创新应用名称</td><td colspan="2">雄安新区建设链金融服务平台</td></tr>
<tr><td>创新应用类型</td><td colspan="2">金融服务</td></tr>
<tr><td rowspan="4">机构信息</td><td>统一社会信用代码</td><td>91130629MA09UT5P4E</td></tr>
<tr><td>全球法人识别编码</td><td>5493001KQW6DM7KEDR62</td></tr>
<tr><td>机构名称</td><td>中国建设银行股份有限公司河北雄安分行</td></tr>
<tr><td>持有金融牌照信息</td><td>牌照名称：中华人民共和国金融许可证
机构编码：B0004L213060001
发证机关：中国银行业监督管理委员会河北监管局</td></tr>
<tr><td>拟正式运营时间</td><td colspan="2">2020 年 08 月 30 日</td></tr>
<tr><td>技术应用</td><td colspan="2">1.在获取建设单位、施工企业、供应商及劳务公司企业的授权前提下，基于区块链技术，依法合规将建设项目中的合同数据、企业数据、付款数据进行上链管理，利用分布式账本的不可篡改特性记录建设资金流动过程，使用区块链智能合约技术实现资金管理的自动化，实现资金拨付留痕、资金基于智能合约规则的自动划拨。
2.基于大数据技术，对链上付款数据进行分析，使财政部门能够更加准确的判断拨付进度是否与项目实施进度相匹配，从而更合理的分配、拨付财政资金。</td></tr>
<tr><td>功能服务</td><td colspan="2">项目运用区块链技术，构建雄安新区建设项目的资金拨付及融资解决方案，基于链上合同数据实现建设项目资金穿透式拨付，保障供应商和工人建设者的资金权益。提供基于链上数据的融资服务，减轻企业融资压力。
1.在建设资金拨付场景中，提供穿透式资金拨付。实现了资金从建设单位到施工企业，再到供应商、劳务公司和工人的层层自动划拨，切实保障农民工和供应商的相关权益。
2.提供基于链上数据的融资服务。在获取授权前提下，依法合规将合同付款数据上链，分析建设项目中各机构的收付款关系链及供应链，基于链上可信数据并以链上应收账</td></tr>
</table>

		款数据为依据，可实现供应商等分包机构的融资服务，助力解决企业融资难题。 3. 通过数据分析辅助决策，为雄安新区建设资金管理带来便利，提供统一管理和决策的依据。 本项目由中国建设银行独立研发与运维。
	创新性说明	1. 实现建设资金穿透式拨付。使用区块链智能合约构建自动化资金拨付机制，大幅减少从资金源到收款方的层层确认流程，实现一键拨付，大幅提高拨付效率。 2. 实现建设资金管理透明化。在合规授权的前提下，所有的资金拨付记录实现区块链上链留痕，资金流公开、透明，更有利于社会监督、政府监管。 3. 实现中小微企业快速融资。基于链上可信的项目数据和拨付数据，为企业融资提供辅助参考，缩短信贷融资周期，助力解决中小微企业融资难题，实现企业融资的精准滴灌。 4. 实现资金、项目管理的高效决策分析。基于区块链上可溯源的资金拨付信息流，结合大数据等技术，为管理者提供便捷的统一管理和决策分析服务。
	预期效果	1. 为项目建设相关供应商、劳务公司提供便利的资金拨付及管理服务，提升项目资金拨付效率。 2. 穿透式资金拨付解决了传统建设资金拨付领域中工人、供应商应收账款被层层克扣的问题，能够切实保障工人建设者和供应商的合法权益。 3. 实现中小微企业快速融资，助力解决中小微企业融资难题。
	预期规模	按照风险可控原则合理确定用户范围和服务规模。预计年服务机构客户数 1 万户，个人客户数 10 万人，年交易笔数 100 万笔，年交易金额 200 亿元，年融资规模 30 亿元。
创新应用服务信息	服务渠道	通过线上渠道提供服务
	服务时间	7×24 小时
	服务用户	建设单位、施工企业、供应商、劳务公司、工程建设者
	服务协议书	《服务协议书-雄安新区建设链金融服务平台-企业服务协议书》
合法合规性评估	评估机构	中国建设银行股份有限公司河北雄安分行内控合规部
	评估时间	2020 年 04 月 29 日

	有效期限	3 年		
	评估结论	项目按照《中华人民共和国合同法》、《中华人民共和国劳动法》、《保障农民工工资支付条例》（中华人民共和国国务院令第 724 号）、《国务院办公厅关于全面治理拖欠农民工工资问题的意见》（国办发〔2016〕1 号）、《商业银行互联网贷款管理暂行办法》、《中国人民银行贷款通则》等进行评估，在数据收集和使用过程中采取措施保护付款信息和用户敏感信息安全，所提供金融服务符合相关法律法规要求，可依法合规开展业务应用。		
	评估材料	《合法合规性评估报告-雄安新区建设链金融服务平台》（见附件 1-1）		
技术安全性评估	评估机构	中国建设银行股份有限公司河北雄安分行信息技术部		
	评估时间	2020 年 04 月 24 日		
	有效期限	3 年		
	评估结论	本项目按照《个人金融信息保护技术规范》（JR/T 0171—2020）、《信息安全技术 信息系统安全保护等级定级指南》（GB/T 22240-2008）、《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《区块链技术金融应用评估规则》（JR/T 0193-2020）、《云计算技术金融应用技术规范 技术架构》（JR/T 0166—2018）、《云计算技术金融应用技术规范 安全技术要求》（JR/T 0167—2018）、《云计算技术金融应用技术规范 容灾》（JR/T 0168—2018）、《金融科技创新安全通用规范》等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。经评估，本项目符合现有相关行业标准要求。		
	评估材料	《技术安全性评估报告-雄安新区建设链金融服务平台》（见附件 1-2）		
风险防控	风控措施	1	风险点	基于区块链的链上数据进行融资的新模式，为银行信贷风险管理带来了挑战，企业授信的额度计算尚无可参考依据，存在过度授信的风险。
			防范措施	在银行业务风险管理方面，保持审慎授信的原则，控制区块链融资规模，建立与新服务模式匹配的授信管理体系和机制，设立专门的区块链风险控制团队对信贷规模及风险进行跟踪评估。
		2	风险	在数据上链存储或读取链上数据时，网络请求可能会被监听、窃取或恶意破坏，可能存在隐私数

			点	据泄露的风险。
			防范措施	严格遵循“用户授权、最小够用、全程防护”原则，在数据收集过程中对数据进行加密及签名验证保护，数据在系统中展示均采用脱敏处理，保护用户隐私数据。使用非对称加密、双通道加密等技术进行数据传输，避免信息被窃取、篡改、恶意破坏，使用加密算法实现区块链数据存储加密，并对敏感数据进行脱敏展示，加强数据在上链及下链场景中的安全管理。
		3	风险点	创新应用上线运行后，可能面临网络攻击、业务连续性中断等方面风险，亟需采取措施加强风险监控预警与处置。
			防控措施	在项目实施过程中，将按照《金融科技创新风险监控规范》建立健全风险防控机制，掌握创新应用风险态势，保障业务安全稳定运行，保护金融消费者合法权益。
		4	风险点	基于应收账款等进行融资，可能存在虚假交易、重复融资风险，例如施工企业与供应商互相串通，伪造交易凭据，虚构应收账款进行融资。
			防控措施	严格交易真实性审核，防范虚增虚构应收账款、存货及重复抵押质押行为。企业在进行应收账款融资时需要提交相关合同凭证及支付凭证至银行融资系统中，银行派专人核实交易信息是否属实，同时通过区块链对企业行为进行存证，一旦发现虚假交易行为，将列入信用黑名单。
	风险补偿机制	建设银行针对可能存在的风险隐患，按照风险补偿方案（见附件 1-3）建立健全风险补偿机制，建立风险赔付等补偿措施，可通过柜面、95533 等渠道提出投诉意见和赔付要求。我行受理后，由牵头业务部门指派相关分行核实情况，确认我行所承担责任，并联系客户，按照客户协议相关约定进行赔付，切实保障金融消费者合法权益。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。		
	退出机制	建设银行按照退出预案（见附件 1-4），在保障用户资金和信息安全的前提下进行系统平稳退出。当满足退出条件时： 1. 业务方面，按照退出方案终止有关服务，及时告知客户		

		并与客户解除协议；如遇法律纠纷，按照服务协议约定进行仲裁、诉讼；涉及资金的，按照服务协议约定退还客户，对客户造成资金损失的通过风险补偿机制进行赔偿。 2.技术方面，由科技部门进行系统下线、版本回退处置。涉及数据的，按照国家及金融行业相关规范要求做好数据清理、隐私保护等工作。	
	应急预案	建设银行按照应急处置预案（见附件 1-5）妥善处理突发安全事件，切实保障业务稳定运行和用户合法权益。在系统上线前，进行全链路压测、容灾演练，对相关操作人员进行应急处置培训；在系统上线后，定期开展突发事件处置演练，确保应急预案的全面性、合理性和可操作性。建立日常生产运行监控机制，7×24 小时实时监控系统运行状况，第一时间对核心链路、接口、功能模块、硬件资源等的异常情况进行告警。一旦发生突发事件，根据其影响范围和危害程度，及时采取有针对性措施进行分级分类处理，视需要及时关闭增量业务，妥善处置受影响的存量业务，切实保障用户资金和信息安全。	
投诉响应机制	机构投诉	投诉渠道	1.营业网点 向营业网点大堂经理、网点负责人反映问题或通过客户意见簿留言。 营业网点名称:中国建设银行容城支行 地址:容城县奥威路 61-1 号 2.客服电话 致电客户服务热线（95533），选择人工服务联系客服代表。 3.门户网站 通过门户网站（http://www.ccb.com.cn）“联系我行”栏目在线留言。 4.网上银行 通过门户网站（http://www.ccb.com.cn）登录个人网上银行，联系我行在线客服。 5.短信银行 将您的投诉内容编辑成手机短信，发送至“95533”。

		投诉受理 与处理机制	我行接受投诉后，投诉会通过建行行内投诉系统流转至建设银行河北省分行金融科技部，技术层面问题由金融科技部受理，业务层面问题由系统指派至所在地区支行受理，客户投诉问题一般会在24至72小时内得到答复及相关处理。
	自律投诉	投诉渠道	受理机构：中国互联网金融协会 投诉网站： https://tousu.nifa.org.cn 投诉电话：400-800-9616 投诉邮箱： fintech_support@nifa.org.cn
		投诉受理 与处理机制	中国互联网金融协会是经党中央、国务院同意，按照人民银行、银监会、证监会、保监会、工信部、公安部、工商总局等10部委联合发布的《关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号）要求，由中国人民银行会同银监会、证监会、保监会等国家有关部委组织建立的国家级互联网金融行业自律组织。为保护金融消费者合法权益，营造守正、安全、普惠、开放的金融科技创新发展环境，协会按照金融管理部门相关要求建立健全消费者投诉处理机制。 对于涉及相关试点地区的金融科技创新应用项目的争议、投诉事项，协会接收投诉意见后，由相关部门依程序进行处置，并接受金融管理部门监督审查。 联系方式：400-800-9616 对外办公时间：周一至周五 上午8:30-11:30 下午13:30-17:00

备注	无
承诺声明	我机构承诺所提交的材料真实有效，严格遵守相关金融管理要求，已全面开展合规性评估和内控审计，能够有效保障业务连续性和用户信息安全，防范资金失窃风险。 以上承诺如有违反，愿承担相应责任与后果。 法定代表人或其授权人（签字）　　年　月　日（盖章）

雄安新区建设链金融服务平台

企业服务协议

《雄安新区建设链金融服务平台企业服务协议》（以下简称“本协议”）由以下双方于____年___月___日在河北雄安新区签署：

甲方：

负责人：

住所：

统一社会信用代码：

乙方（用户）：

法定代表人：

住所：

统一社会信用代码：

鉴于：

1. 双方拟运用“雄安新区建设链金融服务平台”（以下简称“区块链平台”）就乙方参与的_____（以下简称“本项目”）开展区块链平台应用合作。

2. 甲方作为金融机构，经雄安新区改革发展局（以下简称 “新区改发局”）授权，有权就乙方使用区块链平台事宜与乙方签署本协议。

3. 乙方作为区块链平台用户，拟使用“区块链平台”用于本项目款项的收取和支付，并同意遵守本协议内容，接受新区改发局以及甲方的监督和管理。

现甲乙双方在友好协商的基础上，就“区块链平台”使用事宜达成如下协议：

第一条 定义

1.1 “区块链平台”指新区改发局委托中国建设银行开发的雄

安新区建设链金融服务平台，该区块链信息系统具有项目管理、进度管理、资金支付、资金管理及融资等功能。

1.2 鉴于新区改发局委托其他金融机构也开发了建设资金管理区块链信息系统，并且各金融机构开发的信息系统实现了各系统之间的连接。为明确系统开发及运维主体，本协议所指的“区块链平台”特指中国建设银行为新区改发局开发并运营的雄安新区建设链金融服务平台。

第二条 甲方权利义务

3.1 在满足甲方规定的业务办理条件下，甲方应为乙方办理登录区块链平台的银行账户和相关配套业务。

3.2 甲方应及时准确地处理乙方在区块链平台上发送的电子支付指令。

3.3 如果乙方使用的区块链平台开发方和运维方为中国建设银行河北省分行，中国建设银行河北省分行及其分支机构（含甲方）负责该区块链平台的安全、日常运营和维护工作，保证区块链平台的安全运营。

第三条 乙方权利义务

4.1 乙方自愿接受并使用区块链平台，并将其作为本项目唯一收付款路径。

4.2 乙方同意接受区块链平台的管理，按照新区改发局要求如实上传本项目相关信息和证明材料。新区改发局有权在区块链平台上查询包括但不限于乙方的工程信息、交易信息、支付结算信息、履约信息等；乙方同意甲方配合新区改发局查询区块链平台内绑定的银行账户支付结算等信息。

4.3 出现下列任何情况的，新区改发局有权限制乙方区块链平台

用户使用平台功能并要求乙方整改，并有权授权甲方配合其对银行账户功能进行相应管理，直至整改完毕，因整改过程造成的一切后果和损失，均由乙方自行承担：

（1）乙方存在劳资纠纷；

（2）乙方的资质和所提供的相关服务无法满足合同要求；

（3）乙方存在非法转包及违法分包情形；

（4）乙方与上下游客户发生与本项目有关的合同纠纷；

（5）乙方录入平台的工程进度、供应商等相关信息与本项目管理相关的大数据系统内信息存在较大差异；

（6）新区改发局或监管部门认定的，因乙方原因导致本项目存在进度、质量、安全问题；

（7）乙方存在其他违反诚实信用原则或者造成其他不良社会影响的行为。

4.4 乙方对账户内资金的管理应当遵循《雄安新区政府投资项目资金管理暂行办法》（以下简称“暂行办法”）的有关要求，乙方不得通过柜面、ATM、银行网银等渠道规避暂行办法以及区块链平台的统一支付管理。

4.5 乙方基于本项目向甲方提出融资需求时，乙方授权甲方查询乙方本项目交易信息、支付结算、履约等信息。

4.6 乙方了解并同意，乙方有义务保证录入区块链平台的信息的真实性和有效性。如乙方提供的信息不合法、不真实、不准确、不详尽，乙方须承担因此引起的相应责任及后果。

4.7 乙方若为中标联合体牵头单位的，有义务督促中标联合体其他成员、分包商、上下游客户将区块链平台作为本项目唯一收付款路径。

第四条 安全条款

2.1 乙方有义务按照流程向新区改发局申请办理区块链平台上线事宜，由新区改发局为乙方添加主管权限，向乙方发放区块链平台用户名和密码（该用户名和密码是区块链平台用以确认用户身份的唯一有效凭证），并保证区块链平台的使用安全。

2.2 为保证安全使用，乙方应在收到区块链平台的用户名及密码后及时修改密码，并指定专人妥善保管区块链平台的用户名、密码，不得向他人泄露或提供给他人使用。

2.3 乙方主动泄露或遭受他人攻击、诈骗等行为导致的损失及后果，甲方并不承担责任，乙方应通过司法、行政等救济途径向侵权行为人追偿。

2.4 乙方了解并同意，由乙方从区块链平台发出的电子支付指令均代表乙方真实意思表达，甲方均视其为有效指令，并依此执行或进行账务处理，由此造成的一切后果均由乙方负责。

2.5 乙方了解并同意，如果乙方使用的区块链信息系统为甲方及其上级单位所开发和运维，甲方及其上级单位应严格保证该系统的安全，如甲方及其上级单位故意或因重大过失造成区块链平台出现重大安全事故并给乙方造成损失的，甲方应承担赔偿责任，但因服务器、网络故障等客观原因导致乙方损失的，甲方不承担任何责任。

2.6 乙方了解并同意，如果乙方使用的区块链信息系统为其他金融机构所开发和运维，甲方只负责执行从该区块链信息系统发给甲方的电子支付指令，由此造成一切后果由乙方承担。如乙方出现损失，并且认为该损失由其使用的区块链信息系统造成，乙方应向该区块链信息系统的开发方和运维方进行追偿或索赔，甲方不承担任何责任。

第五条 保密条款

5.1 甲方对区块链平台上乙方的信息资料和交易记录等负有保密义务。对前述信息的使用应严格限定在本协议约定范围内，国家法律法规另有规定的除外。

5.2 协议履行过程中，双方不得侵犯对方或第三方的知识产权；在本协议有效期间获知的其他方的商业秘密、技术秘密等需保密的事项，各方均不得向任何第三方披露或公开；国家法律法规另有规定的除外。

第六条 协议的变更与终止

6.1 本协议经双方一致同意后方可变更或补充。协议的变更或补充应以书面方式进行。

第七条 违约责任

7.1 任何一方违反本协议内容，应当按照本协议约定承担相应的责任。

7.2 受损失方有权要求违约方承担违约责任及赔偿因其行为造成的直接损失，并保留依法追究违约方法律责任的权利。

第八条 免责条款

8.1 因战争、自然灾害等不可抗力原因，致使甲乙任何一方无法享有本协议所规定的权利的或无法履行相应的义务的，其他任何一方不因此承担责任，也不享有追索的权利，但双方均应尽其所能减少损失，并在前述情况消除后合理的时间内将处理方案通知其他协议方。

第九条 纠纷处理

9.1 双方在履行本协议的过程中，如发生纠纷，双方应友好协商解决；协商不成时，双方一致约定向甲方所在地人民法院提起诉讼。

9.2 本协议适用中华人民共和国法律。

9.3 如果本协议的部分规定与有关的法律法规相抵触，双方应按有关的法律法规履行自己的权利义务，协议的其他部分的效力不受影响。

第十条 其他条款

10.1 本协议自双方签字盖章之日起生效，至本项目资金支付全部完成之日起终止。

10.2 本协议未尽事宜，可由双方协商签署补充协议，补充协议与本协议具有同等法律效力。

10.3 本协议一式肆份，双方各执两份，具有同等法律效力。

甲方（盖章）:

负责人签字或盖章:

（或授权代理人）

乙方（盖章）:

法定代表人签字或盖章:

（或授权代理人）

签约时间:　　年　　月　　日

附件 1-1

合法合规性评估报告

评估项目名称：雄安新区建设链金融服务平台

评估时间： 2020 年 4 月 29 日

评估意见：

雄安新区建设链金融服务平台，利用区块链智能合约技术等特性实现建设项目中资金的穿透付款，并保证资金支付安全、透明，并使用大数据技术对可信数据进行分析，辅助政府进行决策。

项目按照《中华人民共和国合同法》、《中华人民共和国劳动法》、《保障农民工工资支付条例》（中华人民共和国国务院令第724号）、《国务院办公厅关于全面治理拖欠农民工工资问题的意见》（国办发〔2016〕1 号）、《商业银行互联网贷款管理暂行办法》、《中国人民银行贷款通则》等进行评估，在数据收集和使用过程中采取措施保护付款信息和用户敏感信息安全，所提供金融服务符合相关法律法规要求，可依法合规开展业务应用。

中国建设银行股份有限公司

河北雄安分行内控合规部

2020 年 4 月 29 日

附件 1-2

雄安新区建设链金融服务平台
技术安全性评估报告

日期：2020 年 4 月 24 日

一、摘要

中国建设银行河北雄安分行于 2020 年 04 月 23 日至 2020 年 04 月 24 日对雄安新区建设链金融服务平台相关系统应用进行了安全渗透测试。

渗透测试结果及风险分布图如下:

严重问题: 0 个

中等问题: 0 个

轻度问题: 0 个

安全风险汇总如下:

威胁级别	数量	安全问题名称
严重问题	0 个	
中等问题	0 个	
轻度问题	0 个	

二、项目信息

测试单位信息

单位名称	中国建设银行河北雄安分行信息技术部
项目名称	雄安新区建设链金融服务平台
单位地址	河北省雄安新区容城县奥威路 61-1 号

三、项目概述

3.1 测试目的

通过本项目的成功实施，在坚持科学、客观、公正原则的基础上，全面、完整地了解当前雄安新区网站的安全状况，分析系统所面临的各种风险，模拟攻击者可能利用的漏洞，根据测试结果发现系统存在的安全问题，并对严重的问题提出加固的建议。

本次测试预期达到的目标为:

发现授权渗透测试目标系统的安全漏洞

针对发现的漏洞提供加固方案及防护建议

3.2 测试范围

漏洞类型测试结果如下:

测试分类	测试项	测试结果
web 安全	跨站脚本攻击（XSS）	通过
	sql 注入	通过
	任意目录遍历	通过
	使用 get 方式传送用户名密码	通过
业务逻辑安全	用户弱口令	通过
	业务逻辑漏洞	通过
	用户权限控制	通过
服务器安全	操作系统弱口令	通过
	数据库弱口令	通过

整体而言，系统在本次渗透测试实施期间的安全风险状况为“良好状态”。(系统安全风险状况等级的含义及说明详见附录 A)。

3.3 测试依据

安全测试服务将参考下列规范进行工作。

信息安全技术 信息安全风险评估规范（GB/T 20984-2007）

信息技术 信息安全管理实用规则（GB/T 19716-2005)(ISO/IEC 17799:2000)

信息系统安全风险评估实施指南　　信息系统审计标准（ISACA）

OWASP OWASP_Testing_Guide_v3

OWASP OWASP_Development_Guide_2005

OWASP OWASP_Top_10_2010_Chinese_V1.0

3.4 测试工具

御剑 1.5、BurpSuite、nmap、john the ripper、sqlmap 等。

四、测试过程

4.1web 安全

4.1.1 跨站脚本攻击

4.1.1.1 漏洞描述

跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS) 的缩写混淆，故将跨站脚本攻击缩写为 XSS。恶意攻击者往 Web 页面里插入恶意 Script 代码， 当用户浏览该页之时，嵌入其中 Web 里面的 Script 代码会被执行，从而达到恶意攻击用户的目的。在不同场景下，XSS 有相应不同的表现形式，主要分为反射型、存储型以及 DOM 型的跨站脚本攻击，所造成的影响主要是窃取用户登录凭证（Cookies）、挂马攻击、页面访问挟持等。

4.1.1.2 测试方法

在登录页面，依次对用户、密码输入以下内容进行测试:

'><script>alert(/xxx/)</script><!—

" onerror=alert(/xxx/) t="

" onmousemove=alert(/xxx/) t="

'><img src=# onerror=alert(1)>

'><iframe src=http://www.baidu.com><'

根据返回页面是否弹出包含 xxx 字符串的窗口判定是否存在存储型 XSS;
对其他页面中的输入框使用同样方法进行检测。

4.1.1.3 测试结果

页面提示正常，测试通过。

4.1.2 sql 注入

4.1.2.1 漏洞描述

SQL 注入（SQLi）是一种注入攻击，可以执行恶意 SQL 语句。它通过将任意 SQL 代码插入数据库查询，使攻击者能够完全控制 Web 应用程序后面的数据库服务器。攻击者可以使用 SQL 注入漏洞绕过应用程序安全措施；可以绕过网页或 Web 应用程序的身份验证和授权，并检索整个 SQL 数据库的内容；还可以使用 SQL 注入来添加，修改和删除数据库中的记录。

4.1.2.2 测试方法

使用 sqlmap，测试系统某接口，命令如下:

sqlmap -u "http://www.test.com/api/xxx";

4.1.2.3 测试结果

通过扫描，未发现 sql 注入，测试通过。

4.1.3 任意目录遍历

4.1.3.1 漏洞描述

目录浏览漏洞是由于网站存在配置缺陷，导致网站目录可以被任意浏览，这会导致网站很多隐私文件与目录泄露，比如数据库备份文件、配置文件等，攻击者利用该信息可以为进一步入侵网站做准备。

4.1.3.2 测试方法

在浏览器中，访问项目+任意目录，示例如下:

http://www.test.com/index/resource

http://www.test.com/index/css

4.1.3.3 测试结果

未能成功访问，浏览器返回 404，页面信息不存在，测试通过。

4.1.4 使用 get 方式传送用户名密码

4.1.4.1 漏洞描述

使用 get 的方式传送用户名密码，用户名密码请求信息会展示到地址栏中，很容易被其他人窃取。

4.1.4.2 测试方法

在地址栏中输入登录链接，用户名密码以参数的形式拼到链接后，完整 url 信息示例如下:

http://www.test.com/login?username=xxx&password=123

4.1.4.3 测试结果

未能登录系统，系统保持在登录页面，测试通过。

4.2 业务逻辑安全

4.2.1 用户弱口令

4.2.1.1 漏洞描述

弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险。

4.2.1.2 测试方法

经了解，雄安新区建设链金融服务平台应用新增用户时，密码校验规则为：至少 8 个字符，至少 1 个大写字母，1 个小写字母，1 个数字和 1 个特殊字符，故不存在弱口令。

4.2.1.3 测试结果

测试通过。

4.2.2 业务逻辑漏洞

4.2.2.1 漏洞描述

业务逻辑漏洞是指由于程序逻辑不严谨或逻辑太复杂，导致一些逻辑分支不能正常处理或处理错误。

4.2.2.2 测试方法

权限校验：使用不同角色的操作员登录系统，查看是否有不同资源的访问权限。

1. 使用非建设单位用户登录，是否有：穿透付款发起的权限。

2. 使用非建设单位用户登录，是否有：工资批次新增的权限。

3. 使用建设单位用户登录，是否有：合同新增的权限。

4. 使用非主管角色的用户登录，是否有：用户信息的权限。

4.2.2.3 测试结果

使用不同角色的用户登录，对应权限不同，测试通过。

4.3 服务器安全

4.3.1 操作系统弱口令

4.3.1.1 漏洞描述

SSH 弱口令漏洞指 Linux 系统口令的长度太短或者复杂度不够，如仅包含数字，或仅包含字母等。弱口令容易被破解。攻击者可以利用弱口令直接登录系统，读取甚至修改网站代码。

4.3.1.2 测试方法

使用 hashcat 或者 john the ripper 对系统密码进行扫描破解。

4.3.1.3 测试结果

测试通过，不存在弱口令。

4.3.2 服务器端口扫描

4.3.2.1 漏洞描述

端口扫描是计算机解密高手喜欢的一种方式。攻击者可以通过它了解到从哪里可探寻到攻击弱点。实质上，端口扫描包括向每个端口发送消息，一次只发送一个消息。接收到的回应类型表示是否在使用该端口并且可由此探寻弱点。

4.3.2.2 测试方法

使用 nmap 工具对服务器进行扫描，nmap 命令如下:

nmap -T4 -A -v 1xx.2xx.2xx.1xx

4.3.2.3 测试结果

通过，除应用端口外，未发现其他开放端口。

五、总结

5.1 安全风险总结

5.1.1 安全概况

总体风险描述:

雄安新区建设链金融服务平台应用该应用系统运行环境在当前安全防护体系下未发现3.2小节测试范围内的安全漏洞。

因此，我们认为雄安新区建设链金融服务平台应用的总体安全状态为良好状态。

本项目按照《个人金融信息保护技术规范》（JR/T 0171—2020）、《信息安全技术 信息系统安全保护等级定级指南》(GB/T 22240-2008)、《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)、《区块链技术金融应用评估规则》（JR/T 0193-2020）、《云计算技术金融应用技术规范 技术架构》（JR/T 0166—2018）、《云计算技术金融应用技术规范 安全技术要求》（JR/T 0167—2018）、《云计算技术金融应用技术规范 容灾》（JR/T 0168—2018）、《金融科技创新安全通用规范》等相关金融行业技术标准规范要求进行设计开发并进行全面安全评估。经评估，本项目符合现有相关行业标准要求。

5.1.2 安全管理方面

进一步落实口令管理制度，建议使用独立的、随机生成的满足强度要求的口令，严禁使用弱口令、统一口令管理服务器，及时销毁临时、测试账户；

进一步加强人员安全意识教育，预防攻击事件发生。例如周期性的修改信息系统口令、尽可能的使用客户端收发电子邮件、退出使用 WEB 邮箱系统时一定要注意注销用户而不是关闭浏览器等等；

信息系统上线前增加安全验收环节，保证系统安全上线；

信息系统下线后增加安全退出环境，保证相关信息、防火墙规则、数据的安全处理。

5.1.3 安全技术方面

运行环境部署需要进行加固处理，Web 应用访问数据库的用户需要采用最小权限原则，防止攻击者利用数据库缺陷进行权限提升等操作，同时对中间件软件，如 WEBSPHERE、TOMCAT、JBOSS 等，应进行降权运行处理，防止脚本木马直接获得系统权限；

关注各个应用系统所使用程序、组件、第三方插件等安全现状，及时更新相应的补丁版本，如本次测试过程中所发现的 OWA、jQuery 等；

加强对敏感服务器、配置文件、目录的访问控制，以免敏感配置信息泄露；

加强信息系统安全配置检查工作。

5.1.4 开发过程管理

在系统开发与运行维护的所有阶段（如：计划需求、设计、编码、测试、运行和维护）强制实施严格的变更控制，对变更的申请、审核、测试、批准、执行计划与具体实施提出明确要求，确保系统安全性与控制措施不被损害；

变更控制包括以下内容：

审查变更控制措施和流程的完整性，确保未被修改和破坏；

确保操作系统的更改不会对应用系统的安全性和完整性造成不良影响；

确保系统文档在每次修改后得到及时更新，并确保旧文档被正确归档和处置；

做好软件升级的版本控制，如保存历史版本；

保留所有变更的审计跟踪记录；

确保操作文档以及用户程序能在必要时被修改；

确保及时更新业务连续性计划。

针对开发人员对源代码的管理，应严禁将源代码信息上传至互联网上的网络磁盘或源代码仓库，如 GITHUB、网盘等；建议建立自运营的代码管理仓库，如有必要上传至互联网上，应对敏感关键信息进行屏蔽，如 API 地址、IP 地址、数据库密码等，防止信息泄露；

应尽量避免修改厂商提供的软件包，如必须修改，应注意以下几点：

评估软件包内置的控制措施和完整性流程遭受破坏的风险；

应征得原厂商的同意，由原厂商提供标准的升级程序来实现软件包的更改。

在软件的原始采购、开发、使用和维护过程中，应采取如下防范控制措施：

仅从信誉卓著的厂商处购买软件；

尽量购买提供源代码的软件，以便进行检验，在投入使用之前检查所有源代码；

使用通过权威机构评估测试的软件产品；

一旦安装完毕，控制对源代码的访问和修改；

安装并正确使用有关后门、特洛伊代码的检测和查杀工具。

5.1.5 安全架构设计原则

在应用系统软件开发设计的过程中，对应用系统的总体设计应当满足如下安全原则：

原则	说明
最小权限原则 **Least Privilege**	应用软件的每个模块如进程、用户只能访问当下所必需的信息或者资源。赋予每一个合

	法动作最小的权限，以保护数据以及功能避免受到错误或者恶意行为的破坏。
权限分离原则 **Separation of Duties**	对业务的操作、管理和审计权限应该由软件中的不同角色的用户分别承担；普通用户和管理员用户信息应该存放在不同的数据表中。
深度防御原则 **Defense in Depth**	在应用程序对业务数据进行处理的每个阶段都要考虑安全性问题，不能仅在某个阶段做安全防御，这样单点防御一旦被突破将造成安全风险。
容错保护原则 **Fail Secure**	当程序出现故障时或系统异常导致失败时，可以进入到一个失败保护的状态。如果用户请求失败，系统仍可保障安全。
单点异常终止原则 **Single Point of Failure**	当用户提交数据超出预期时，应立即终止程序的执行，不要试图加以修正并继续执行下去。
外来代码安全原则 **Least Third Party Components**	严格控制第三方函数与插件的使用，对外来代码必须进行详细的安全测试。
代码重用原则 **Leveraging Existing Components**	尽可能的重用软件已有的模块，这样可以降低引入新的漏洞和攻击界面的可能性。
数据保护原则 **Data Protection**	对用户数据的保护功能应涵盖用户数据存储的完整性、用户数据传输保密性、数据传输的访问控制、剩余信息的保护、数据反转操作等内容；应对系统中关键数据（如用户密码等）的存储和网络传输时应采用加密保护，实用加密算法应该符合国际标准、国家标准和业界标准。
可审计原则 **Auditing**	在应用系统中设计审计日志记录的功能，并对应用系统产生的日志增加完备的审计功

	能。
开放设计原则 **Open Design**	开放设计与“不开放即安全”的原则相对而言，认为设计本身不应具有神秘感。这一原则的具体表现可以参见应用于加密设计的 Kerchoff 定律，“系统不应单纯依赖私密性，若落入敌人手中则毫无优势可言”；开放设计以提高系统兼容性和可扩展性。
抗抵赖原则 **Anti Repudiation**	对于涉及支付交易等重要的业务场景，系统设计应有效地防止通信双方抵赖，如采用电子证书签名等方式。
规范性 **Standardization**	系统设计所采用的安全技术和安全产品应符合国际标准、国家标准和业界标准，为系统的扩展升级、与其他系统的互联提供良好的基础。
可扩展性 **Scalability**	以当前业务安全需求为基础，充分考虑发展的需要，安全功能模块子系统以插件或接口方式以方便未来的扩展。
实用性 **Practicable**	安全功能设计需要尽可能的考虑投入产出比，同时尽量控制对用户体验的影响。
符合性 **Regulatory Compliance**	安全功能的设计尽可能的要符合国家规范、行业规范以及业界的通用标准，如等级保护等规范。

附录 A. 安全风险状况等级说明

安全风险状况说明	
良好状态	信息系统处于良好运行状态，没有发现或只存在零星的低风险安全问题，此时只要保持现有安全策略就满足了本系统的安全等级要求。

预警状态	信息系统中存在一些漏洞或安全隐患，此时需根据评估中发现的网络、主机、应用和管理等方面的问题对进行有针对性的加固或改进。
严重状态	信息系统中发现存在严重漏洞或可能严重威胁到系统正常运行的安全问题，此时需要立刻采取措施，例如安装补丁或重新部署安全系统进行防护等等。
紧急状态	信息系统面临严峻的网络安全态势，对组织的重大经济利益或政治利益可能造成严重损害。此时需要与其他安全部门通力协作采取紧急防御措施。

附录 B. 漏洞等级状况说明

安全风险状况说明	
低危漏洞	对系统造成较小的影响，攻击成本高，攻击场景较为苛刻，不会直接影响到系统的正常运行，攻击者可能无法通过该漏洞获得权限。
中危漏洞	对系统造成一般的影响，攻击成本一般，在特定场景下将可影响系统的正常运行，攻击者需要配合其他安全漏洞方可间接获得权限。
高危漏洞	对系统造成严重的影响，攻击成本低，一般情况下可直接利用而无需特定场景和要求，攻击者可直接利用该漏洞获得权限。

附件 1-3

雄安新区建设链金融服务平台
风险补偿方案

雄安新区建设链金融服务平台基于区块链等技术，在建设资金支付场景中提供资金穿透支付服务，切实保障农民工和供应商的相关权益，资金支付留痕，利于政府及社会监督，利用数据辅助决策能够为建设资金管理带来便利，提供统一管理和决策的依据，为打造“雄安质量”保驾护航。平台充分考虑相关参与方权益保护工作相关要求，充分尊重平台涉及各方的合法权益，并在执行过程中高度重视风险防控工作，主动履行相关方权益保护义务。

一、客户可通过柜面、95533 等渠道提出投诉意见和赔付要求，对雄安新区建设链金融服务平台的有关客户投诉问题或事项，由当地建设银行网点所属管辖行处理。各业务职能部门根据所辖业务与产品，负责提供相关业务解释工作。

二、造成用户资金损失情况时，由牵头业务部门指派相关分行核实情况，确认我行所承担责任并联系客户，按照客户协议相关约定进行赔付，切实保障金融消费者合法权益。对于非客户自身责任导致的资金损失，提供全额补偿，充分保障消费者合法权益。

三、处理原则

1. 雄安新区建设链金融服务平台是面向建设项目相关方及社会公众全面展示建设银行金融科技水平和金融服务能力的重要平台。客户的服务体验和评价是检验我行综合服务能力的重要依据。各级机构各司其职，责任到人，确保向客户提供高水准的技术维护服务和金融服务体验。

2. 建立雄安新区建设资金区块链平台客户投诉快速响应机制。为确保客户投诉及时、高效处理，建立雄安新区建设链金融服务平台联系人机制，做好各类客户投诉的问题核查与支持保障，及时发现问题、改进问题，不断提升服务能力和服务水平。

附件 1-4

雄安新区建设链金融服务平台
退出预案

雄安新区建设链金融服务平台运用区块链技术，构建建设项目资金拨付及融资的完整解决方案，基于链上合同数据实现建设项目资金穿透式拨付，保障供应商和工人建设者的资金权益，提供基于链上数据的融资服务，减轻企业融资压力。雄安新区建设链金融服务平台在保障用户资金和信息安全的前提下，根据试点情况及监管意见执行后续处理措施，可对项目下线处理、业务部门与合作企业经协商终止协议、开发中心做版本回退、废除相关功能。如有相关法律纠纷，按照合同约定进行仲裁、诉讼，进行平稳退出。

一、 技术退出

（一）数据处理

完成平台相关业务数据、交易数据等信息的数据库归档备份，将用户数据同步到相关业务系统，确保用户其他业务不受影响。

（二）资源回收

回收平台相关的系统资源，包括服务器、 数据库、基础组件等，关闭合作方网络白名单，确保银行系统核心区域的网络安全。

二、 业务退出

（一）履行约定

根据合作双方所签署的相关协议中约定的期限，告知用户，存量业务在规定时间内到期有序退出。

（二）业务调整

按照与相关方确定的整改计划，基础系统按时关闭用户流量，不再新增用户交易。所有合作方完成流程关闭后，下线相关业务。

附件 1-5

雄安新区建设链金融服务平台
应急处置预案

一、目的

为规范雄安新区建设链金融服务平台的安全稳定运行，促进建设项目资金顺利支付，项目工程建设如期推进，保护客户合法权益，建立健全雄安新区建设链金融服务平台的应急工作机制，增强应对和处理重大事项和突发危机的能力，明确应对信息系统和网络的突发事件处理流程，提高员工应对信息系统和网络突发事件的处理能力，规范员工对信息系统和网络突发事件的处理行为，有效防范应急处理风险，特制定本办法。

1. 适用范围

本应急预案适用于雄安新区建设链金融服务平台和网络突发事件的应急管理。

2. 定义

本应急预案所指信息系统和网络突发事件，是指突然发生，出现的影响系统切换目标的操作错误、准备不充分、数据导入不成功、人员意外、公共关系意外等突发事件对平台服务提供方和平台使用方造成或者可能造成严重危害，需要采取相应的应急处置措施予以平息的事件。

二、管理流程

1. 突发事件应急措施管理原则

及时发现，果断行动原则：应该及时掌握情况，果断采取措施，最大程度地减少危害和损失，要遵循以快速高效反应为重点、以正面宣传、积极应对为策略、以保障营业、防范风险为核心、以稳定市场、稳定客户为目标。

统一指挥，协调配合原则：全行要在突发事件处置领导小组的指导下，各专业小组协调联动，立足全方位正面宣传，综合开展各类有效措施积极应对，务求达到快速反应、业务连续、安抚客户、降低影响的目的。

依法处置，稳妥缜密原则：由于建设资金支付与区块链产品新技术的特殊性、复杂性，金融风险的扩散、蔓延往往十分迅速。因此，应该坚持依法有序处置、积极稳妥填密的原则，防止风险进一步扩散和蔓延。

2. 突发事件的级别规定

根据突发事件的情况，按照技术分类标准将突发事件从高到低共分为三个等级；

一级：因特别重大突发事件引发的，计算机信息系统全部瘫痪；

二级：因重大突发事件引发的,计算机信息系统部分瘫痪；

三级：因突发事件引发的，计算机信息系统不能正常运行（业务子系统出现故障）。

随着突发事件的发展，影响范围和程度变化，突发事件的级别可以被提升或降低。

3. 应对突发事件的措施规定

突发事件发生后，产品领导小组及业务落地分行要根据风险级别从后台、前台两个方面采取多项措施积极应对，要求迅速恢复营业，并做好向客户的解释工作。

需要说明的是，因突发事件使得信息系统在其对应的 RTO/RPO 要求时间之内不能恢复正常业务运行时，即须上升为“灾难"，启动灾难恢复计划予以应对。

3.1 后台处置

具体的处理措施包括:

当三级突发事件发生时，迅速启动相关等级的应对预案，采取以下措施:

·主机出现故障：因特殊原因主机出现故障，不能正常运行，应迅速启用备用机，同时对主机进行检查和维修。

·业务子系统出现故障：因特殊原因各业务子系统出现故障，应迅速启用各业务子系统应急预案。

·通讯出现故障：因特殊原因通讯网络出现故障，应立即组织维修。

当二级突发事件发生时，应迅速启动应急预案，采取以下措施:

•生产机房部分受损：如发生因洪水、火灾等自然或人为灾害，生产机房部分不能正常运转的情况，应采取如下措施:

•机房受损:启用同城灾备机房.同时对生产机房进行检查和维修，同城生产机房、灾备机房同时受损：启用异地灾备机房。

•通讯网络部分受损：因网络故障或病毒等原因，导致主线路通

讯瘫痪，应迅速启用备用网络，同时对通讯网络进行检查和维修。

当一级突发事件发生时.应迅速启动应急预案，采取以下措施:

•生产机房全部受损：如发生因洪水、火灾等自然或人为灾害，生产机房不能正常运转的情况，应采取如下措施:

•机房受损：启用同城灾备机房，同时根据受损情况对生产机房进行维修;

•同城生产机房、灾备机房同时受损：启用异地灾备机房。

•通讯网络全部受损：因网络故障或病毒等原因，导致主线路通讯瘫痪，应迅速启用备用网络，同时根据网络具体情况进行维修。

3.2 前台处置

突发事件发生后，突发事件处置领导小组要及时将事件原因和风险级别分别向相关业务部门通报。如果是自然灾害或者人为因素造成的突发事件，信息科技部要及时向安全保卫部通报情况；相关部门负责人和主管业务行领导要认真组织好前台的客户服务工作和相应的安全保卫工作。具体的应对措施包括:

做好客户的解释安抚工作。确认能在短期内可以恢复营业的，应通过在手机客户端线客服或 95533 客服引导客户、安抚客户；不能确认恢复营业时间的，如线下可以办理，可安排客户到线下网点办理业务，线下无法办理的业务及时向客户说明解释。

4. 应急计划的宣传、培训和演习的规定

加强对突发事件应急处置工作的宣传教育工作,负责人与业务小组的安全意识和防范能力，将有关应急方面的法律、法规和应急自救

知识作为宣传教育的内容定期或不定期地对有关应急处置指挥管理机构和单位管理人员进行技术培训和应急演练，保证应急处置预案的有效实施，不断提高突发事件的应急处置能力。

5. 应急计划的维护机制规定

5.1 应急处置机制

应该确保应急处置不会因为技术问题而导致应急响应中断或延长应急处置时间。

应该确保应急处置不会因为物资保障问题而中断。

应该储备一定数量的应急设备和应急物资，保证物资供应渠道畅通。

应该建立预警平台确保应急事件及时被发现并及时传达相关人员。应每季度对第三方是否能够提供及时有效的技术保障进行确认。

应有明确的应急管理部门、岗位的联络方式，包括第三方联系方式和联系电话，并做到及时更新，应有多种联系方式。

5.2 应急计划演练

应该制订应急演练计划，明确应急演练时间、内容、依据、目的、负责人和相关部门。

应急演练内容应该全面完整，涵盖信息系统的各类应急场景。

应该在应急演练中验证预案各个环节是否有效，应急资源是否完备，应急人员是否胜任。

应该控制应急演练引起的信息系统变更风险，避免因演练导致服务中断。

应急演练应该选择在非主要业务时段进行。

应该至少每年进行一次全面的应急演练。

应该每季度对应急演练相关人员进行培训。

5.3 应急演练总结

应急演练结束后，应该撰写应急演练总结报告，大型或重要的应急演练总结报告应提交管理层。

总结报告内容应该包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、改进的措施及实施计划、演练结论。

应该根据演练总结报告提出改进措施并进行整改，及时修订相应的应急预案。

应该组织审计部门对整改情况进行监督和检查。

应该根据审计要求以及监管部门检查要求，将应急演练计划、过程记录和结果分析等归档留存。

5.4 应急计划评审

应该每年至少应对各种突发事件进行一次评估，评估内容包括：风险识别、措施的有效性、预案是否完备、演练是否完备、及时等。

应该每年至少开展一次对应急响应工作的全面评估和审计，评估重点包括：响应和报告是否及时.资源是否充分.

5.5 应急计划变更

应急计划变更流程应该由相关技术人员通过分析，向信息系统应急计划领导小组提出修改意见，由业务恢复小组提出修改方案，上报

应急计划工作小组复核，经应急计划领导小组批准后，进行修订。

如果发生文档资料修改，或外包商更换，也相应该调整信息科技应急计划。