合同编号：JYZX2025003

贵阳市公共资源交易中心年度信息安全服务项目合同

2025年2月

贵阳市公共资源交易中心年度信息安全服务项目服务合同

甲方(用户单位)：贵阳市公共资源交易中心

法定代表人：郑卫城

地址：贵州省贵阳市观山湖区中天会展城SOHO写字楼G座通信

邮政编码：550081

乙方(供应商)：贵阳块数据城市建设有限公司

法定代表人：姚磊

通信地址：贵州省贵阳市高新区长岭南路阳关大道28号中国·西部高新技术研发生产基地1、2、3、4号楼(3)1单元15层、16层

邮政编码：550081

一、服务项目

1.项目名称：贵阳市公共资源交易中心年度信息安全服务项目

乙方向甲方提供贵阳市公共资源交易中心信息安全服务项目(以下简称“本项目”)的信息安全服务。

2.服务地点：贵州省贵阳市。

3.服务内容：本项目服务内容包括：☐系统运维；☑信息安全；☐网站维护；☐链路及硬件租用；☐机房及硬件设备运维；☐云资源；☐密码应用；☐其他服务：驻场运维。

服务内容明细详见《贵阳市公共资源交易中心年度信息安全服务项目服务内容》(附件1)。

4.服务周期：自合同签订之日起一年。

二、合同总金额

本项目合同含税总金额为人民币：柒拾万叁仟元整(小写：¥703,000.00元)。其中不含税金额663,207.55元，税额39,792.45元。

三、付款方式

合同服务期内甲方对乙方履约验收两次，履约验收不合格的，甲方有权解除合同、不支付费用、追究乙方违约责任。合同签订后完成前六个月运维服务期后，组织对服务期前六个月履约验收，验收通过后，乙方提出付款申请，甲方自收到乙方向甲方开具增值税普通发票之日起三十个工作日内，向乙方支付本项目合同金额的50%，计人民币：【叁拾伍万壹仟伍佰元整】（计：【¥351,500.00】元）；服务期满后，组织服务期后六个月履约验收，验收通过后，乙方提出付款申请，甲方自收到乙方向甲方开具增值税普通发票之日起三十个工作日内，向乙方支付剩余50%合同金额，计人民币：【叁拾伍万壹仟伍佰元整】（计：【¥351,500.00】元）。

四、甲方的权利义务

1.甲方的权利

(1)甲方有权随时向乙方了解项目进度，并要求乙方提供项目相关资料。

(2)甲方有权按照本合同约定或有关法律法规、政府管理的相关职能规定，对本项目进行监督和检查，有权要求乙方按照监督检查情况制定相应措施并加以整改。

(3)甲方有权在乙方履行合同过程中出现损害公共利益、公共安全情形时终止本合同。

(4)甲方是本项目的使用主体，有项目验收、提出完善服务等权利。

(5)甲方有权对项目服务实施过程进行监督管理，一旦发现乙方提供的服务达不到本合同约定要求的，甲方有权要求乙方及时采取改正、修复、更换、重做等补救措施；如乙方未及时补救的，或补救后仍达不到甲方要求，甲方有权按照费用明细扣除乙方费用。

(6)甲方有权根据本项目合同范围内服务内容适时合理地提出服务要求，乙方根据实际情况在合理的时间范围内完成。

2.甲方的义务

(1)甲方应按照本合同的约定向乙方支付合同价款。

(2)甲方应及时向乙方提供与履行本合同相关的且甲方有权提供的必要文件、资料。

(3)甲方应为乙方履行本合同过程中需要的沟通、协调提供必要的协助。

(4)甲方应根据乙方提交的验收申请，按时组织相关单位进行验收。

五、乙方的权利义务

1.乙方的权利

(1)乙方有权按照本合同约定向甲方收取合同价款。

(2)乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料，经鉴定，因甲方未提供导致乙方无法履行合同义务的，乙方不承担责任。

(3)乙方有权申请甲方协调，为乙方履行本合同项下服务提供必要的协助。

2.乙方的义务

(1)乙方根据本合同要求开展项目服务工作。

(2)乙方应建立健全服务应急处置机制，保障系统日常稳定运行。

(3)乙方应自觉接受甲方对项目运维、资金使用情况等的督查检查。

(4)乙方应积极配合甲方对本项目服务水平和质量的评估工作。

(5)按照“保持安全、管理、技术并重，分权制衡，最小特权”的总体方针和“预防为主”的基本方针，协助甲方加强信息系统安全保护管理工作，包含不仅限于协助建立系统日常运维管理机制、协助建立数据安全运维管理机制、协助完善本地机房安全管理等信息系统安全相关工作。

六、验收

1.验收主体

甲方对乙方提供的服务进行验收。

2.验收方式和验收标准

验收方式和验收标准依照按国家相关标准、地方要求、本项目实施方案、响应文件、合同等的规定执行。

3.验收流程

甲方在收到乙方验收申请后30个工作日内进行验收并出具验收意见，未验收合格的，乙方完成相关整改后重新提交验收申请，直至通过验收为止。

七、知识产权

1.本合同生效后，在本合同项下所提供服务产生、获取的数据(若有)，乙方未经甲方书面同意不得授权第三方使用数据。

2.双方在本合同生效前，本合同项下所提供的服务以外，以及双方在服务中运用其自身技术、经验，或公共技术与信息所获取或产生的技术成果，其全部知识产权仍归双方各自所有。本合同生效后，在本合同项下所提供服务形成的所有知识产权归属于甲方所有。

3.乙方保证对所提供的软硬件产品及附属设施、技术资料具有合法产权或已取得合法授权，不存在侵犯他人合法权利的情形。如有除合同之外的第三方向甲方主张侵权，乙方应出面解决，因此造成的损失，由乙方承担。

八、保密条款

1.乙方应遵守国家有关保密的法律法规和行业规定，落实保密措施，并确保合作过程中涉及的国家秘密、业务需求文件、协议、系统设计、技术成果等内容和相关事务的保密安全。未经甲方书面同意，不得将承接本项目获得的政府、公民个人等各种信息和资料提供给其他无关的单位和个人。如发生以上情况，甲方有权索赔并追究乙方法律责任。

2.本合同保密条款长期有效，无论本合同是否生效、被撤销、变更、解除或终止，各方仍应执行本合同保密条款。

九、安全生产及安全管理

1.甲方应向乙方传达贯彻国家和有关部门制定的安全生产方针、政策、法规、制度，并做好安全管理和监督检查工作。

2. 甲方应经常深入项目现场掌握安全生产情况，针对不安全因素提出改进措施。

3. 甲方应在合法合规方式下使用与本合同相关服务，如因违反国家、地方现行规定(相关规定)而导致乙方受损失时，甲方应承担全部责任。

4. 乙方认真执行“安全第一，预防为主”的工作方针，遵守执行甲方的各项规章制度。

5. 乙方单位在录用施工人员时，必须严格按照国家的有关规定，
不得聘用不适应行业以及不能胜任项目要求的员工。

6. 乙方作业人员应遵守操作规程，不违章指挥、不违章作业、不违反劳动纪律。

7. 乙方对高空作业，多层次同时作业，必须有可靠防护措施。

8. 乙方应建立信息安全管理制度和措施，按照《中华人民共和国网络安全法》等法律法规以及政务信息系统安全管理等有关规定实施。

9. 如在提供服务中发生重大安全事故及安全隐患的，乙方必须及时上报甲方。

10. 经鉴定后，若属于乙方过错责任导致甲方受损失时，乙方应承担全部责任。

十、违约责任

1. 乙方无正当理由未能按照本合同约定的服务时间提供具体服务或完成约定的具体项目服务内容的，从逾期之日起每日按具体逾期未完成内容所对应的服务费（具体费用明细见附件《贵阳市公共资源交易中心信息安全服务项目服务内容》的报价明细表）0.01%的标准向甲方支付违约金，但因甲方需求变更、因甲方导致实施条件不完备、政策变化或客观情况发生重大变化等造成延期的，乙方不承担逾期违约责任。

2. 甲方无正当理由未能按照合同约定按时足额支付合同款的，从逾期之日起每日按应付未支付合同款的0.01%的数额向乙方支付违约金。如甲方超过90个工作日未及时付款，乙方有权暂停服务，由此产生的一切后果及责任，乙方不承担相关责任。

3. 任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件发生后及时向另一方通知，以减轻可能给另一方造成的损失，在取得有关机构的不可抗

力证明或谅解确认后，允许相应延期履行或修订合同，并可根据具体情况部分或全部免于承担违约责任。由于不可抗力导致合同不能履行的，任意一方均有权终止合同。

4. 甲、乙双方应遵循诚实信用原则，按照合同约定充分履行合同义务，保障合同顺利履行完毕。若因非可归责于双方的原因导致项目提前终止，双方另行商定解决方案，防止产生国有资产投资风险及损失。

5. 除本合同另有约定外，发生违约情形，违约方应赔偿由此给另一方造成的一切损失。如属双方过错，应各自按过错承担相应责任。因一方违反本合同约定构成违约，另两方提起诉讼维护自身合法权益的，有权要求违约方承担由此造成的包括但不限于律师费、诉讼费、保全费、诉讼保全责任保险保函费、执行费、公告费、及必要的交通住宿费等。该费用的承担不影响违约方承担其他违约责任或损失赔偿责任。

十一、争议解决

本合同在履行过程中发生的任何争议，如双方不能通过友好协商解决，任何一方可通过甲方所在地有管辖权的人民法院诉讼处理。除有关争议的条款外，在争议的解决期间，不影响本协议其他条款的继续履行。

十二、通知与送达

1.根据本合同需要发出的全部通知，均须采取书面形式，以(1)专人递送，(2)特快专递，(3)传真，(4)挂号信件发出。特快专递或挂号信件的交寄日以邮戳为准。上述书面通知均须标明合同各方为收件人。

2.上述书面通知按对方在本合同中所列的地址发出，如任何一方的地址有变更时，须在变更前10日以书面形式通知对方。因迟延通知而造成的损失，由过错方承担责任。未说明的，一方按照合同约定地址通知的，视为已经履行送达义务，未说明方由此遭受的损失自行承担。

3.双方将按如下规定确定通知被视为正式送达的日期：

(1)以专人递送的，接收人签收之日视为送达；

(2)以传真方式发出的，以发件方发送后打印出的发送确认单所示时间视为送达；

(3)以特快专递形式发出的，发往本市内的，发出后第3日视为送达。

(4)以挂号方式发出的，发往本市内的，邮寄后第3日视为送达。

十三、其他

1.双方确定，在本合同有效期内：

(1)甲方指定项目联系人及联系信息如下：

姓名：刘娴；

职务：工作人员；

电话：0851-84839757

地址：贵州省贵阳市观山湖区中天会展城SOHO写字楼G。

(2)　乙方指定项目联系人及联系信息如下：

姓名：沈小珊；

职务：项目经理；

电话：0851-84877999；

地址：贵州省贵阳市高新区长岭南路阳关大道28号中国·西部高新技术研发生产基地1、2、3、4号楼(3)1单元15层、16层；

开户行：贵阳农村商业银行科技支行；

开户名称：贵阳块数据城市建设有限公司；

账号：820000000001391849。

(3)任何一方变更项目联系人的，应当及时以书面形式通知另外一方。

2.本合同自双方法定代表人或授权代表签字并加盖公章或合同专用章之日起生效。

3.本合同所有附件均为合同的有效组成部分，与本合同具有同等法律效力。

4.本合同一式陆份，具有同等法律效力，甲方执肆份，乙方执贰份。

5.本合同未尽事宜，由甲乙双方另行签订补充协议，与本合同具有同等法律效力。补充协议条款与本合同不一致的，以补充协议为准。

附件1:贵阳市公共资源交易中心信息安全服务项目服务内容；

附件2:保密协议

附件3:验收标准

（以下无正文）

（本页无正文，为签章页）

甲 方（盖 章）： 贵阳市公共资源交易中心

法定代表人或授权代表（签字/签章）：

经办人：

2025年 2月19 日

乙 方（盖 章）： 贵阳块数据城市建设有限公司

法定代表人或授权代表（签字/签章）：

经办人：

2025 年 2月 17 日

附件1:贵阳市公共资源交易中心信息安全服务项目服务内容

一、运维服务

提供5名人员通过驻场运维服务方式配合现场运维服务方式提供12个月的安全风险评估、漏洞扫描、渗透测试服务、安全通报服务、安全加固服务、重要时期安全保障、网站安全云监控、安全巡检服务、应急响应服务、安全攻防演练、新系统入网安全评估、舆情监控服务，完善信息安全制度，加强系统网络安全防护，建立及时可靠的信息安全管理机制，为贵阳市公共资源交易中心电子交易系统安全提供有效的保障，具体服务内容如下：

1.1 安全风险评估

1.1.1 服务简介

网络安全风险评估是对网络和业务系统的安全漏洞、安全隐患、安全风险，进行探测、识别、控制、消除的全过程，它从风险管理角度，运用科学的方法和手段，系统地分析网络与应用系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。

网络安全评估的内容，包括网络拓扑架构、安全域规划、边界防护、安全防护措施、核心设备安全配置、设备脆弱性等，从而全面评估网络的安全现状，查找安全隐患。

1.1.2 评估内容

1.1.2.1 资产评估

信息资产的识别可以确定评估的对象，是整个安全服务工作的基础。并且，本阶段可以帮助交易中心实现信息资产识别和整理，完成一份完整和最新的信息资产清单，对交易中心的信息资产管理工作会有所帮助。

首先识别信息资产，完成所有重要信息资产的清单。按照资产性质和业务类型等可以分成若干资产类，一般分为数据，软件，服务，硬件，设备和文档等。根据不同的项目目标与项目特点，重点识别的资产类别会有所不同，在通常的项目中，一般数据、软件和服务为重点。

1.1.2.2 架构安全评估

对网络结构，逻辑网络结构及网络的关键设备进行评估，发现存在的安全性方面的问题。结合业务体系、系统体系等结构的检查逻辑网络，由什么物理网络组成以及网络的关键设备的位置所在对于保持网络的安全是非常重要的。另外，鉴定关键网络拓扑，对于成功地实施一个基于网络的风险管理方案是非常关键的。基本信息包括网络带宽，协议，硬件（例如：交换机，路由器等）Internet 接入，地理分布方式和网络管理。发现网络结构存在的安全性问题。

1.1.2.3 配置安全评估

对网络及安全设备的配置进行检查，对 IP 地址分配是否正确、VLAN 划分是否合理，路由协议、安全策略是否合理等多方面进行分析，网络配置是整个网络安全的基础。

发现网络设备配置存在的不合理及安全性问题。

1.1.2.4设备漏洞扫描

为了充分了解交易中心当前网络存在的安全隐患，采用综合漏洞评估扫描工具对交易中心的网络进行全面扫描，检查其网络设备的弱点，识别被入侵者用来非法进入网络的漏洞。

通过对交易中心的网络设备的扫描，发现目前交易中心网络设备存在的技术性安全漏洞。同时，也为安全加固工作提供依据。

首先，确定扫描范围，主要针对重要信息资产和抽样网段。然后提交扫描方案和扫描申请，明确扫描执行人员和时间安排。采用骅阜综合漏洞评估扫描工具对网络进行全面扫描，检查其网络设备的弱点，识别被入侵者用来非法进入网络的漏洞。

1.1.3服务频次

根据甲方需要，每年至少开展两次全面的网络安全风险评估工作，服务周期一年。

1.2漏洞扫描

1.2.1服务简介

在网络安全体系的建设中，安全扫描工具花费低、效果好、见效快，与网络的运行相对独立，安装运行简单，要以大规模减少安全管理的手工劳动，有利于保持全网安全政策的统一和稳定，是进行风险分析的有力工具。

本项目安全扫描主要是通过评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据库、应用软件和用户帐号/口令等安全对像目标存在的安全风险、漏洞和威胁。服务对象主要中心业务系统和服务器。漏洞扫描的详细服务范围如下：

➢操作系统

Windows、发行版 Linux、AIX、UNIX 通用、Solaris 等主流操作系统。

➢数据库

Oracle、MySQL、MSSQL、Sybase、DB 等主流数据库。

➢常见应用服务

Apache、IIS、Tomcat、Weblogic 等主流应用服务，常见 FTP、EMAIL、DNS、TELENT、POP3、SNMP、SMTP、Proxy、RPC 服务等。

➢Web 应用程序

ASP、PHP、JSP、NET、JZVA、Python、Shell 等语言编写的 WEB 应用程序。

➢网络设备

常见的路由器、交换机等设备。

1.2.2 扫描内容

安全漏洞扫描会对信息系统内的网络设备、操作系统、应用软件、中间件和服务等进行安全漏洞识别，详细内容如下。

1.2.2.1 系统层安全

该层的安全问题来自网络运行的操作系统：UNIX 系列、Linux 系列、Windows 系列以及专用操作系统等。安全性问题表现在两方面：一是操作系统本身的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是操作系统的安全配置存在问题。

●身份认证：例如通过 Telnet 进行口令猜测等

●访问控制：注册表 HKEY_LOCAL_MACHINE 普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录

●系统漏洞：操作系统本身存在各类漏洞问题

1.2.2.2网络层安全

该层的安全问题主要指网络信息的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入、路由系统的安全、入侵检查的手段等。

网络资源的访问控制：检测到无线访问点。

域名系统：ISCBINDSIG资源记录无效过期时间拒绝服务攻击漏洞，WindowsDNS拒绝服务攻击。

路由器：ciscoIOSWeb配置接口安全认证可绕过，路由器交换机采用默认密码或弱密码等。

1.2.2.3应用层安全

该层的安全考虑网络对中心提供服务器所采用的应用软件和数据的安全性，包括：数据库软件、WEB服务、电子邮件、域名系统、应用系统、业务应用软件以及其它网络服务系统等。

数据库软件：Oracle、Mysql、MSSQL等帐号弱口令问题。

WEB服务：SQL注入攻击、跨站脚本攻击、基于WEB的DOS攻击。

电子邮件系统：Sendmail头处理远程溢出漏洞，Microsoft Windows SMTP服务认证错误漏洞。

为了确保扫描的可靠性和安全性，首先制定扫描计划。计划主要包括扫描开始时间、扫描对象、预计结束时间、扫描项目、预期影响、需要对方提供的支持等等。

在实际开始评估扫描时，评估方会正式通知项目组成员。服务商按照预定计划，在规定时间内进行并完成评估工作。如遇到特殊情况（如设备问题、停电、网络中断等不可预知的状况）不能按时完成扫描计划或致使扫描无法正常进行时，由双方召开临时协调会协商予以解决。

1.2.2.4漏洞响应

对漏洞扫描结构生成漏洞扫描报告，报告内容报告漏洞在系统中的存在点，产生漏洞的主要原因，漏洞的修复建议和加固意见。安全工程师在实施安全漏洞扫描服务过程中，严格按照安全服务的流程，在现场进行安全扫描方案实施漏洞扫描后，会在两个工作日（需根据扫描对象的数量进行实际调整）内出示一份漏洞扫描报告。报告名称如下：

《××系统安全漏洞扫描报告》《××IP漏洞扫描报告地址段安全漏洞扫描报告》

1.2.3服务频次

每月进行依次漏洞扫描，服务服务周期一年。

1.3渗透测试服务

1.3.1服务简介

渗透测试服务，是在交易中心授权的前提下，以模拟黑客攻击的方式，对交易中心业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。

在渗透过程中，我们会采用业界领先的漏洞检测技术、攻击技术、攻击工具。

过程分为四步：计划与准备、信息收集、实施渗透、输出报告。计划与准备阶段主要是根据网站反馈的内容制定项目实施方案与计划；信息收集与实施渗透是项

目的实施阶段，输出报告主要是汇总和评估项目中发现的安全威胁，并输出文档。

1.3.2测试内容

对市交易中心网站的渗透测试，除使用产品和工具扫描外，更重要的需要进行人工渗透，渗透内容包括但不限于以下项，且需要对发现的漏洞进行验证和利用。

序号	渗透测试大项	渗透测试小项
1	配置管理	备份测试、HTTP方法测试、传输安全
2	身份鉴别	用户注册、账户权限、账户枚举、弱口令
3	认证授权	认证绕过、目录遍历、授权绕过、权限提升
4	会话管理	超时测试、会话管理绕过测试、会话令牌泄露测试、跨站点请求伪造CSRF测试
5	输入验证	SQL注入、代码注入、命令执行注入、跨站脚本XSS
6	错误处理	错误码分析、栈追踪分析

7	业务逻辑	数据验证、请求伪造、完整性、次数限制、上传测试

1.3.3服务频次

渗透测试服务每年两次，服务周期一年。

1.4安全通报服务

1.4.1服务简介

信息安全是动态发展的，面对日益演变的安全攻击手段和系统安全漏洞的不断发现和利用，信息系统面临的风险也在不断变化。实时关注安全动态，了解最新的安全技术、安全事件、安全风险能够提高交易中心的整体信息安全。

安全通告服务提供及时、准确的anql风险预警，第一时间通知交易中心，并提供专业的安全解决建议。

1.4.2服务内容

服务商凭借国内领先的安全研究能力，广泛的采集途径，和全球同步的安全信息收集系统，使我们能将最新最严重的安全问题，最快的通报给中心并且给出相应的解决办法，从而大大减轻网管人员做安全技术追踪和分析的压力。服务商的安全通告服务将下面的这些成果与中心共享。

提供安全通报对象范围包括：

➢常见厂商的软、硬件网络设备：思科、华为等路由、交换设备；

➢常见厂商的操作系统：微软、惠普、苹果、IBM等操作系统；

➢常见厂商的数据库软件：微软MSSQL、甲骨文Oracle等；

➢常见厂商的Web软件：BEAWeblogic、IBMWebsphere、Apache、JBoss、Tomcat。

安全通告提供最新安全漏洞、威胁、0day、网络攻击、勒索病毒等关键的安全咨询，并提供安全建议。安全通告服务具体内容由以下模块组成：

➢公告ID：CVE编号；

➢公告标题：漏洞名称；

➢厂商：漏洞涉及的厂商；

➢发布时间：漏洞发布时间；

➢受影响软件及系统：漏洞影响的软件及系统；

➢综述分析：对漏洞进行描述，同时分析其造成影响的原因；

➢解决方法：厂商补丁发布的链接；若厂商还未发布相应的补丁，根据安全问题的实际情况，提供暂时的解决方案。

1.4.3 服务频次

安全通告服务每月一次，服务周期一年，有重大安全事件时，随时通知。

1.5 安全加固服务

1.5.1 服务简介

为了有效保障网络的安全运行，在对操作系统、中间件、网络设备、安全设备进行安全检测后，需要对发现的安全风险进行修复。

安全加固服务，是指根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、中间件、网络设备、安全设备，都需要进行安全加固。

1.5.2 加固内容

1.5.2.1 操作系统加固内容

服务商可进行安全加固的操作系统包括 Windows、Linux、AIX、HP-Unix、Solaris。操作系统的加固内容如下表所示，详细的加固列表可参见服务商的操作系统安全加固规范。

序号	加固大项	加固小项
1	账号管理和认证授权	账号、口令、授权、关机设置
2	协议安全配置	IP协议安全、防火墙、SYN攻击防护
3	服务和共享配置	系统服务、默认共享、共享权限
4	日志安全配置	日志审核策略、日志文件设置
5	其它安全配置	空闲超时设置、自动播放、启动项、数据执行保护

1.5.2.2 数据库安全加固

服务商可进行安全加固的数据库系统包括 Oracle、SQLServer、DB2。数据库的加固内容如下表所示，详细的加固列表可参见服务商的数据库安全加固规范。

序号	加固大项	加固小项
1	账号管理和认证授权	账号、口令
2	通信协议安全	网络数据传输安全、信任IP设置
3	日志安全配置	数据库审核策略、数据库日志文件设置
4	其它安全配置	连接超时设置、监听器密码

1.5.2.3 中间件安全加固

服务商可进行安全加固的中间件系统包括 Tomcat、Apache、WebLogic、WebSphere。中间件系统的加固内容如下表所示，详细的加固列表可参见服务商的中间件安全加固规范。

序号	加固大项	加固小项
1	账号管理和认证授权	账号、口令
2	通信协议安全	启用https传输、更改tomcat默认端口
3	日志安全配置	日志记录设置
4	其它安全配置	登录超时、错误重定向、禁止显示文件

1.5.2.4 网络设备安全加固

服务商可进行安全加固的网络设备包括主流厂商的路由器、交换机。网络设备的加固内容如下表所示，详细的加固列表可参见服务商的网络设备安全加固规范。

序号	加固大项	加固小项
1	账号管理和认证授权	账号管理、登录安全要求、认证授权
2	通信协议安全	SNMP协议安全、路由协议安全、IP协议安全
3	日志安全配置	日志记录设置
4	其它安全配置	关闭不必要的服务、端口

1.5.2.5安全设备安全加固

服务商可进行安全加固的安全设备是主流厂商的防火墙，如Juniper、天融信、CiscoASA等。安全设备的加固内容如下表所示，具体的加固列表可参见服务商的安全设备安全加固规范。

序号	加固大项	加固小项
1	账号管理和认证授权	账号、口令、授权
2	访问控制安全	安全策略、远程管理
3	日志安全配置	启用本地日志、启用远程日志
4	增强安全要求	限定管理IP、更改默认Banner、设备自身安全设置

1.5.3服务频率

通常情况下，每月进行一次安全加固服务。发布重大安全漏洞时，也需要立即进行安全加固。

1.6重要时期安全保障

1.6.1服务简介

重要时期安全保障，是指国家及省级重大活动、重大会议等特殊时期内，服务商派出安全攻防经验丰富的安全专家，进驻市交易中心，对目标系统进行安全值守和保障，对业务系统的安全状况进行实时监控和日志分析。

在安全保障期间，当目标遭受黑客入侵攻击时，值守人员立即对入侵事件进行分析、检测、抑制、处理，查找入侵来源并恢复系统正常运行，完成后给出应急响应报告，报告中将还原入侵过程，同时给出对应的解决建议。

1.6.2服务频率

国家法定假日、国家及省、市级重大活动、重大会议等特殊时期，按业主方指定提供安全保障服务。

1.7网站安全云监控

1.7.1服务简介

随着互联网技术的快速发展，网站攻击的门槛不断降低。各类型网站受到的安全威胁越来越多，为形象、各 Web 应用系统的正常使用。应实现以下基本安全需求：

- 监控网站页面内容完整、不被篡改；
- 监控网站存在的 SQL 注入、XSS、非法访问、信息泄露等应用层漏洞，从而提前解决潜在风险；

- 监控网站，防止网站挂马而导致的中心满意度损失；
- 监控网站是否存在敏感信息，对于网站的敏感信息内容自行配制告警功能，方便管理者及时了解到发生的安全事件，可根据量化的标准，对网站的安全事件严重程度进行不同形式的告警，杜绝可能存在的政治风险和声誉损失；
- 监控网站是否被钓鱼，导致相关的名誉损失。

服务商针对政府网站的高要求部署一套全天候 Web 监测系统，统基于 SAAS（软件即服务）模式，通过部署于各信息节点的监测引擎对中心指定的网站（WEB 应用）进行可用率和站点安全性检测，以保障中心网站业务持续性，从而向中心提供网站安全的保障。

1.7.2服务频率

网站网站安全进行7*24小时监控，出现紧急情况时，立即通知业主。

1.8安全巡检服务

1.8.1服务简介

信息安全是动态的，随着时间的变化会不断暴露出新的安全漏洞、恶意软件、攻击手段，新些将打打破现有信息安全的平衡。安全风险管理是一个持续性的过程，安全巡检服务是安全风险管理过程中的重要组成部分。

服务商的安全巡检服务，是指定期对中心网站进行的安全检测，检测完成后提供全面的巡检服务报告，给出存在的安全风险并提供对应的修复建议。

1.8.2服务内容

1.8.2.1安全漏洞评估

采用服务商漏扫及国际上著名的漏洞扫描工具，对市交易中心信息系统进行漏洞扫描，查找信息系统上存在的安全漏洞，完成后给出详细的漏洞扫描报告，报告中包括漏洞修复建议。

1.8.3安全日志审计

对防火墙、IPS、WAF 等产生的安全日志进行收集，综合对这些日志进行关联分析，从多个维度对目标的运行状态进行分析，得出一段时间内目标系统及相关设备的安全运行状态。

1.8.4 服务频率

对市交易中心信息系统的安全巡检，每月 1 次，全年共 12 次。

1.9 应急响应服务

1.9.1 服务简介

应急响应服务是为满足交易中心发生安全事件，需要紧急解决问题的情况而提供的一项安全服务。当交易中心发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，服务商安全专家会在第一时间对安全事件进行应急响应处理，使交易中心的信息系统在最短时间内恢复正常运行，帮助交易中心查找入侵来源，为交易中心挽回或减少经济损失。

对安全事件进行应急响应处理后，我们将提供详细的应急响应报告，报告中将还原入侵过程，同时给出对应的解决方案。

1.9.2 服务频率

出现安全事件时，立即进行应急响应，服务商 2 小时内赶到业主指定地点，服务周期为 1 年。应急响应结束后 5 个工作日内出具应急响应报告。

1.10 安全攻防演练

1.10.1 服务简介

安全问题“三分技术、七分管理”，作为安全管理的主要执行者-人员，在面临信息安全威胁的严峻挑战时，提高安全意识和安全技能，成为了一项必要的工作。然而，掌握信息安全技术对人员的实践要求很强，目前市面上大部分安全培训均偏重于理论，很难有效提升受训人员的技术水平。

攻防演练可以为中心提供一个理论结合实际的、可上机演练实践的、可放心操作动手、场景真实生动逼真的网络安全攻防实验环境，从而提升受训人员的技术和动手能力，对于进行网络信息安全建设和培养合格的网络信息安全技术人才具有重要的意义。

1.10.2 服务频率

每年开展一次，服务周期为 1 年。

1.11 新系统入网安全评估

1.11.1 服务简介

通常，对于业务系统的安全评估，可分为入网前安全评估和在线安全评估两种方式，从业务系统的角度出发，两种方式的影响分析如下。

评估影响 / 评估方式	入网前安全评估	在线安全评估
风险	较小，无业务压力	大，有业务压力
技术难度	小	大，影响在线业务
整改成本	较小，整改由开发商承担	大，需要立项整改
可操作性	强	较弱

新系统在入网前进行安全评估，不论是风险、技术难度、整改及可操作性等方面都有较大优势。同时，政策法规也要求，新系统在入网前，必须进行安全风险评估。

新系统入网安全评估，包括渗透测试、漏洞检测、从而评估新系统的安全状况，查找不符合安全要求的配置项以及安全风险点。

1.11.2 评估内容

1.11.2.1 渗透测试

模拟黑客攻击的方式，对新系统应用层面的安全漏洞进行全面检测，查找应用层面的安全隐患和隐患，评估新系统的安全状态并提供漏洞修复建议。

渗透测试，除使用产品和工具扫描外，更重要的需要进行人工渗透，渗透内容包括但不限于以下项，且需要对发现的漏洞进行验证和利用。

序号	渗透测试大项	渗透测试小项
1	配置管理	备份测试、HTTP方法测试、传输安全
2	身份鉴别	用户注册、账户权限、账户枚举、弱口令
3	认证授权	认证绕过、目录遍历、授权绕过、权限提升
4	会话管理	超时测试、会话管理绕过测试、会话令牌泄露测试、跨站点请求伪造CSRF测试
5	输入验证	SQL注入、代码注入、命令执行注入、跨站脚本XSS
6	错误处理	错误码分析、栈追踪分析
7	业务逻辑	数据验证、请求伪造、完整性、次数限制、上传测试

1.11.2.2漏洞检测

对新系统进行系统漏洞检测，包括操作系统漏洞检测、数据库漏洞检测、中间件漏洞检测，并给出漏洞修复建议。

- **操作系统漏洞检测**

采用DPtechScanner漏洞扫描系统，对新建系统的所有操作操作系统进行安全漏洞检测，查找操作系统中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

- 数据库漏洞检测

采用DPtechScanner漏洞扫描系统，对新建系统的所有数据库进行安全漏洞检测，查找数据库中的安全隐患和安全隐患，并给出对应的漏洞修复建议。

- 中间件漏洞检测

采用DPtechScanner漏洞扫描系统，对新建系统的所有中间件进行安全漏洞检测，查找中间件的安全隐患和安全隐患，并给出对应的漏洞修复建议。

1.11.3服务频率

新系统入网前进行，按需提供。

1.12舆情监控服务

1.12.1服务简介

服务商应根据中心具体需求，提供舆情监控服务，发现互联网，客户端、抖音，小红书等关于贵阳市公共资源交易中心的舆情监测服务。

1.12.2服务内容

服务商可根据中心具体需求，提供必要的技术支持咨询服务。咨询范围将包括但不限于以下内容。

➢ 全网动态监测，全天候对新闻媒体、SNS 媒体、非主流门户网站、论坛、QQ 公众号、短视频等多个平台的社会舆论舆情展开监测，当前和过去在网络上出现了什么随时掌控。

➢ 舆情预警，透过智能化语法识别，可识别脆弱等正面讯息，并积极支持透过 QQ、短信、电子邮件或者应用程序等多种不同舆情预警方式，提醒延后最快 30 秒内。

➢ 舆情分析，可对舆情展开全面性综合分析，包括舆情追根溯源、舆情散播媒体、网站、Pudukkottai、情感倾向分析、舆情散播趋势分析等。

➢ 舆情报告，舆情分析结果信息化、统计图表化，可将监测和分析过程中的信息、讯息和工具栏便捷加入到控制系统，手动生成舆情会议记录，并积极

支持自动求出，拥有专业领域舆情分析师团队，透过定性及定量，多维度、多维度地分析总结舆情讯息散播特点及规律，提供更多专业领域网络舆情报告。

1.12.3 服务频率

按月提供舆情监控报告，突发舆情在 3 小时内出具舆情监控报告，并出具出具处置建议。服务周期为 1 年。

二、费用明细

序号	服务内容	数量（次）	单价（元）	总价	服务标准
1	安全风险评估	2	￥45,000.00	￥90,000.00	包括资产评估、架构安全评估、配置安全评估、设备漏洞扫描，每年2次，上下半年各一次。
2	漏洞扫描	12	￥5,000.00	￥60,000.00	主要是通过评估工具对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据库、应用软件和用户帐号/口令等安全对像目标存在的安全风险、漏洞和威胁。服务对象主要中心业务系统和服务器并出具漏洞扫描报告。每月一次
3	渗透测试服务	2	￥30,000.00	￥60,000.00	对交易中心业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。每年2次，上下半年各一次。
4	安全通报服务	12	￥4,000.00	￥48,000.00	安全通告提供最新安全漏洞、威胁、0day、网络攻击、勒索病毒等关键的安全咨询，并提供安全建议。每月一次。
5	安全加固服务	12	￥6,500.00	￥78,000.00	安全加固服务，是指根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、中间件、网络设备、安全设备，都需要进行安全加固。每月一次。
6	重要时期安全保障	一年内按需提供，至少8次	￥8,000.00	￥64,000.00	重要时期安全保障，是指国家及省级重大活动、重大会议等特殊时期内，派出安全攻防经验丰富的安全专家，进驻市交易中心，对目标系统进行安全值守和保障，对业务系统的安全状况进行实时监控和日志分析。按需，每年不少于8次。

7	网站安全云监控	11	￥3,000.00	￥33,000.00	7*24 小时监控，部署一套全天候 Web 监测系统，统基于 SAAS（软件即服务）模式，通过部署于各信息节点的监测引擎对中心指定的网站（WEB应用）进行可用率和站点安全性检测，以保障中心网站业务持续性，从而向中心提供网站安全的保障。按照11个系统预估。
8	安全巡检服务	12	￥5,000.00	￥60,000.00	包括安全漏洞评估、安全日志审计，每月一次。
9	应急响应服务	一年内按需提供	￥30,000.00	￥30,000.00	出现安全事件时，立即进行应急响应，2小时内赶到业主指定地点，按需。
10	安全攻防演练	1	￥45,000.00	￥45,000.00	采用真实、模拟等手段开展攻防演练，每年1次。
11	新系统入网安全评估	一年内按需提供，至少1次	￥15,000.00	￥15,000.00	包括安全风险评估、渗透测试、漏洞扫描等，预估每年至少1个新系统，1次服务。
12	舆情监控服务	12	￥10,000.00	￥120,000.00	根据中心具体需求，提供舆情监控服务，发现互联网，客户端、抖音，小红书等关于贵阳市公共资源交易中心的舆情监测服务，每月一次，突发舆情在 3 小时内出具舆情监控报告。
合计		**￥703,000.00**			
投标总报价大写：柒拾万零叁仟元整，小写：703,000.00元					

附件 2

保密协议

甲方： 贵阳市公共资源交易中心
乙方： 贵阳块数据城市建设有限公司

鉴于甲方与乙方正就“贵阳市公共资源交易中心年度信息安全服务项目”（项目编号为：MCHC-DZ--ZG20248127）进行合作，甲方可能会向乙方披露其保密信息。为了保护双方的利益，确保保密信息的安全，甲乙双方经协商一致，达成以下保密协议：

第一条 保密信息的定义

1.1 “保密信息”指甲方在合作过程中向乙方披露的所有非公开信息，包括但不限于技术资料、商业计划、用户信息、财务数据等。

第二条 保密义务

2.1 乙方同意对甲方披露的所有保密信息保密，并仅在合作项目范围内使用这些信息。

2.2 乙方不得将保密信息泄露给任何第三方，除非该第三方已与甲方签订了保密协议且征得甲方同意，并且该第三方的使用范围仅限于本次合作项目。

2.3 乙方应采取所有合理的措施保护保密信息的安全，包括但不限于限制访问、加密存储和安全传输。

第三条 保密期限

3.1 本协议的保密期限自双方签字之日起至项目结束之日起五年。

3.2 保密期限届满后，乙方仍需对保密信息中的商业秘密继续保密，直至该信息公开。

第四条 违约责任

4.1 如乙方违反本协议的保密义务，乙方应赔偿甲方因此遭受的一切损失。

4.2 赔偿范围包括但不限于直接经济损失、间接经济损失、诉讼费用、律师费用等。

第五条 法律适用与争议解决

5.1 本协议的订立、解释、执行和争议解决均适用中国境内法律。

5.2 因本协议引起的任何争议，双方应首先通过友好协商解决；协商不成时，任何一方均可向甲方所在地的有管辖权的人民法院提起诉讼。

第六条 其他

6.1 本协议的任何修改和补充均需双方书面同意。

6.2 本协议一式陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

甲方（盖章）： **乙方（盖章）：**

签订日期： 年 月 日

附件3

项目验收标准

一、验收内容及阶段

1.项目验收:完成贵阳市公共资源交易中心年度信息安全服务项目工作内容。

2.服务验收:项目每阶段履约验收服务期届满后，乙方形成《安全服务总结报告》及项目开展过程印证材料等验收资料，乙方向甲方提交服务验收申请。

二、验收标准

本项目采用现场验收方式验收,验收标准以符合采购文件参数、响应文件内容、各项要求行业标准、合同约定及甲方其它要求为准。双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由验收小组根据招标文件、投标文件以及合同中质量要求和技术指标进行比较，以有利于甲方利益的标准进行验收。若验收不通过，乙方应根据甲方要求进行整改，整改完成后再次提请验收。由此产生的一切费用由乙方自行承担。

三、验收人员

由甲方组织相关人员参与。

四、项目验收前提条件

1.服务完成内容与采购文件、响应文件及合同约定内容描述一致且所有服务均已按要求完成。

2.根据服务内容准备充分各环节过程资料。

五、项目验收标准

序号	服务内容	服务标准	交付物
1	安全风险评估	包括资产评估、架构安全评估、配置安全评估、设备漏洞扫描，每年2次，上下半年各一次。	《资产登记台账》 《安全风险评估报告》
2	漏洞扫描	主要是通过评估工具对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据库、应用软件和用户帐号/口令等安全对像目标存在的安全风险、漏洞和威胁。服务对象主要中心业务系统和服务器并出具漏洞扫描报告。每月一次	《漏洞扫描报告》
3	渗透测试服务	对交易中心业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。每年2次，上下半年各一次。	《渗透测试报告》 《渗透测试复测报告》
4	安全通报服务	安全通告提供最新安全漏洞、威胁、0day、网络攻击、勒索病毒等关键的安全咨询，并提供安全建议。每月一次。	《安全预警报告》
5	安全加固服务	安全加固服务，是指根据安全加固列表，对目标系统的安全漏洞对进行修复、配置隐患进行优化的过程。安全加固是保证设备和系统安全运行的关键防护措施，通常情况下，操作系统、中间件、网络设备、安全设备，都需要进行安全加固。每月一次。	《基线检测报告》 《基础加固报告》
6	重要时期安全保障	重要时期安全保障，是指国家及省级重大活动、重大会议等特殊时期内，派出安全攻防经验丰富的安全专家，进驻市交易中心，对目标系统进行安全值守和保障，对业务系统的安全状况进行实时监控和日志分析。按需，每年不少于8次。	《重保方案》 《值班表》 《重保终结报告》
7	网站安全云监控	7*24 小时监控，部署一套全天候 Web 监测系统，统基于 SAAS（软件即服务）模式，通过部署于各信息节点的监测引擎对中心指定的网站（WEB应用）进行可用率和站点安全性检测，以保障中心网站业务持续性，从而向中心提供网站安全的保障。按照11个系统预估。	《云监测报告》
8	安全巡检服务	包括安全漏洞评估、安全日志审计，每月一次。	《巡检过程记录》
9	应急响应服务	出现安全事件时，立即进行应急响应，2小时内赶到业主指定地点，按需。	《据实提供《应急响应报告》

10	安全攻防演练	采用真实、模拟等手段开展攻防演练，每年1次。	《演练方案》 《演练过程及总结》
11	新系统入网安全评估	包括安全风险评估、渗透测试、漏洞扫描等，预估每年至少1个新系统，1次服务。	《资产登记台账》更新 《入网安全风险评估报告》
12	舆情监控服务	根据中心具体需求，提供舆情监控服务，发现互联网，客户端、抖音，小红书等关于贵阳市公共资源交易中心的舆情监测服务，每月一次,突发舆情在 3 小时内出具舆情监控报告。	《舆情监控报告》
	共性材料	/	用户报告
		/	《驻场人员考勤》及驻场过程记录
		/	安全服务总结报告