附件1

项目采购需求及评分标准

1. **项目管理及服务需求**

为进一步加强深圳市地方金融监督管理局网络安全防护水平，落实深圳市党政机关网络安全工作要求，及时掌握单位网络安全现状，促进网络安全制度、安全责任的落实，完善安全防护措施，建立健全信息化管理体系，提升网络安全管理水平，保障网络环境、信息系统安全有效运行，不断提升机关安全管理水平和安全防护水平，项目服务内容具体如下：

|  |  |  |
| --- | --- | --- |
| **服务名称名称** | **服务内容** | **服务周期** |
| **一、资产登记造册台账** | 终端资产登记造册需包含：计算机主机名、IP地址、MAC地址、使用人或责任人姓名、所属部门、物理位置；对外服务的服务器私有IP与互联网IP的对应表，切实做到资产清、底数明。 | 全年 |
| **二、网络安全管理体系建设服务** | 1.网络安全管理体系建设顾问咨询，传递、培训国际网络安全管理体系标准及最新进展，分析本单位的组织架构、业务要求，以及信息系统的特点，确定IT安全目标，建立安全组织架构，进行风险分析，并依据风险分析结果选择控制措施。  2.根据法律法规、安全标准、管理需求建立网络安全管理体系，以网络安全工作为重点，将网络安全融入日常运营管理，以制度化推动机关信息化运维管理水平。根据本年度护网行动、全市党政机关网络安全联合检查等文件精神，修订完善机关网络安全管理制度。  3.建立网络安全自审自查机制，使用文件调阅、现场调研、人员访谈、基线分析的方式，确定现有的安全管理制度与实际要求的管理制度之间存在的差距与不足，按照网络安全管理制度制订方法，对现有的安全管理制度进行修订。 | 全年 |
| **三、信息系统网络安全等级保护顾问咨询服务** | 1.根据《信息安全技术 网络安全等级保护定级指南（GB/T 22240-2020）》为机关信息系统等保测评和定级提供自测、调试、整改、报评等工作，协助完成等保测评工作并取得等保测评报告和定级报告。  2.根据信息系统等级保护的相关要求，对所有新信息系统开展上线前安全检测，并对检测中发现的安全漏洞给出修复建议，协助开展漏洞修复工作，对已修复的漏洞进行验证。新系统上线前安全检测的内容包括以下几项：主机层安全扫描、应用层安全扫描、操作系统安全策略检查、应用系统安全策略检查等。 | 每年一次 |
| **四、网络安全风险评估服务** | 对机关的网络及信息系统进行风险评估（信息资产核查、威胁识别等），依据指标分析现有安全状况及基本差距，出具风险评估报告及差距分析报告，并提出整改建议**。** | 每年一次 |
| **五、安全漏洞隐患检测评估服务** | 每季度对所有终端、服务器、信息系统、网站等开展安全漏洞检测评估工作，针对检测中存在的安全漏洞，由服务单位协助各系统开发单位完成漏洞整改，并根据市主管部门的要求按照时间节点上报安全检测报告。 | 每年4次 |
| **六、信息系统漏洞修复加固服务** | 建立操作系统、终端等IT设备或系统安全基线规范，根据建立的安全基线规范提供基线核查服务，定期对信息系统、服务器、终端协助进行漏洞修复和配置加固。 | 全年 |
| **七、渗透测试服务** | 根据全市网络安全绩效考核、党政机关事业单位网络安全联合检查指标要求及《深圳市电子政务信息安全管理试行办法》规定，依据安全渗透性测试标准和方法，配合已经发现的安全漏洞，在用户的授权下，模拟入侵者的攻击方法对应用系统、服务器系统和网络设备进行非破坏性质的攻击性测试，直观地暴露自身网络所面临的威胁与风险点。渗透测试的基本步骤包括：信息收集、制定测试策略、对已知漏洞进行测试、对漏洞进行验证、挖掘目标未知漏洞、获取和提升权限、扩大渗透范围。 | 每年2次 |
| **八、安全监测管理服务** | 1.资产管理服务：定期采用资产梳理专用工具提供主机各类信息（端口、网站、Web容器、第三方组件、进程、账号）的梳理服务，通过分析信息资产变动情况，帮助用户审计主机资产历史变动，发现异常资产行为。服务完成后按照变更日期形成《信息资产登记表》。  2.安全体检服务：定期采用安全体检专用工具对主机发起深度检测服务，检测的项目包括系统漏洞、弱口令、高危账号、配置缺陷、异常账号、异常进程、系统命令校验。通过安全体检服务让用户能够看得懂安全，对主机存在的风险一目了然。服务完成后提交《系统安全体检报告》。  3.安全监控服务：针对服务范围内内网主机服务器提供各类安全监控服务，从主机安全角度，全天候监控主机的运行情况，包括登录监控、完整性监控、操作审计、进程监控、资源监控、性能监控，能确保第一时间发现服务器问题，可通过短信或邮件形式进行告警，快速发现安全风险和性能瓶颈。  4.入侵威胁检测服务：展示及处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件包括：病毒木马、网页后门、反弹shell、异常账号、日志异常删除、异常登录、异常进程、本地提权、网络蜜罐诱捕、内存马检测、系统命令校验、进程监控、异常shell命令、文件和账号异常操作、文件蜜罐、后门监测、异常外联等行为检测。  5.安全防护服务：根据信息系统特性提供端口安全防护、暴力破解防护、扫描防护、病毒防护、IP限制设置、进程控制等服务，对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件。 | 全年 |
| **九、终端安全专项检查服务** | 根据全市网络安全绩效考核要求，由服务单位定期对我局终端开展安全检查服务，检查内容包括密码、屏保、系统补丁、防病毒更新和标识粘贴情况。根据检查结果，针对不符合要求的，现场配合终端用户开展安全整改工作。 | 每年一次 |
| **十、网络安全事件应急体系建设及应急演练服务** | 1.根据《深圳市网络安全事件应急预案（修订稿）》，以及国家、省、市等网络安全主管部门相关政策要求，结合我局网络安全现状和需求，对现有的网络安全事件应急预案进行审核，修订和完善《深圳市地方金融监督管理局网络安全事件应急预案》（以下简称《应急预案》），并进行审核确认。应急预案包括但不限于以下内容：总则、组织机构与职责、监测与预警、应急响应、事件分级分类、响应流程、后期处置、应急保障、宣传培训和演练。  2.开展网络安全突发事件应急演练，形成演练材料（包括：演练方案、演练脚本、参与人员、相关视频图片、总结报告及改进措施等）。 | 每年一次 |
| **十一、网络安全意识教育培训服务** | 网络安全意识主要指非专业网络安全工作人员需要了解的日常网络安全相关知识和技能。网络安全意识培训主要包括但不限于办公电脑、平板、智能设备、移动存储设备等终端设备在使用互联网、内网网络的安全、保密意识和安全常识，由服务单位制定网络安全培训计划，确认培训内容及培训方式，通过开展全员网络安全培训，提高全体工作人员的网络安全意识。 | 每年一次 |
| **十二、重点时期网络安全保障服务** | 在重要节日、重大活动、护网行动（深蓝、粤盾等）等重保时期提供网络安全保障，做好网络安全隐患排查、安全防护、预警监测等安全保障技术支撑服务，确保业务系统安全运行，避免敏感事件或影响业务的安全事件发生。 | 全年 |
| **十三、网络安全检查服务** | 按照我市网络安全绩效考核评估工作及我市党政机关事业单位网络安全联合检查要求开展我局网络安全体系建设及防护工作，具体内容如下：  1、网络安全绩效考核工作：网络安全重大事件防范情况、统筹协调和规范开展网络安全检查、组织开展应急演练、网络安全风险和网络安全事件处置反馈情况。  2、网络安全联合检查迎检工作：安全管理组织、人员管理、安全制度落实、安全合规、安全防护措施落实、应急体系建设、安全教育培训、信息系统等保测评、安全隐患排查及整改。  3、内部网络安全检查工作：成立安全检查工作组，制定并印发安全检查相关文件；召开网络安全检查专题会议；制订网络安全检查方案，并对自查工作进行过督导；进行网络安全检查结果通报；编写网络安全检查总结报送市联合检查组。  4、完成上级单位下发的工作任务：根据市网络安全主管单位下发的文件，研讨文件内容和要求，落实文件中布置的各项网络安全工作任务，认真总结，找出不足，持续改进，并根据文件要求，及时将工作开展情况和整改情况上报。 | 每年一次 |
| **十四、网络安全应急响应支持服务** | 服务单位提供7x24小时重大安全事件的应急响应服务，在我局发生网络安全事件时第一时间现场协助进行处置，采取有效的措施尽快恢复网络、信息系统、终端电脑的正常运行，处置完成后输出应急处置报告。包括但不限于对计算机病毒事件、蠕虫病毒事件、特洛伊木马事件、网页内嵌恶意代码事件、拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、信息篡改事件、信息假冒事件、信息窃取事件等网络安全事件应急响应工作。 | 全年 |
| **十五、网络安全顾问咨询服务** | 提供安全咨询支持，担任网络安全的咨询顾问，在网络、主机和信息系统进行升级、扩建时，提供安全顾问咨询服务，和信息安全评估服务，并根据实际情况提供咨询服务解决方案等。  作为咨询顾问，需要提供全方位的咨询服务，通过电话、E-mail、现场研讨等方式，协助对信息系统中出现的安全问题或与安全相关的问题进行处理。 | 全年 |
| **十六、供应链安全管理支持服务** | 协助对供应链安全管理工作，包含完善供应链安全管理制度、供应商管理、供应商人员管理、应急响应等 | 全年 |

**（二）项目服务要求**

2.1项目总体要求

1、根据单位实际情况编写项目总体安全服务方案，对各项工作的内容、方法、时间进行描述，其中工作时间以周为单位进行量化；

2、每季度进行一次网络安全运行现状分析，详细描述本月信息安全工作开展情况进行总结、列出存在的安全隐患，以及提出整改建议。并书面呈报；

3、对在项目实施中需要协调和协助的工作，将至少提前一周书面通知，以便有充分的时间安排时间和业务协调；

4、项目实施中所有的文档：过程数据、会议纪要、过程文档、计划、方案、策略等，将以电子、纸质同时保存（至少一式两份存档），随时接受检查；

5、针对不同的工作内容实行文档（电子及纸质）分类管理，文档分类要清晰，容易调阅。每项工作完成后都有相应的工作附件与之呼应；

6、项目实施中对信息系统采用的任何技术检测（本地核查、网络扫描、安全分析、设备调研）手段和方法，将事先提交详细的实施（检测）方案，明确检测内容、方法、使用的规则（策略）、可能引发的后果、以及后果的处理等内容，经确认通过后才进行实施；

7、按时完成本年度网络安全联合检查工作各阶段要求的上报材料（如，工作计划、实施方案、核查表等）并准时提交；

2.2应急响应要求

将提供7\*24小时服务，在发生故障需要提供技术支持时，保证能够联系上相关服务人员。

在出现紧急事件时，接到报告后，以最快的速度(1小时内)派遣安全技术工程师到达现场，协助进行处理， 技术支持人员在解决故障时，要最大限度保护好数据，做好故障恢复的文档，力争恢复到故障点前的业务状态。对于“系统瘫痪，业务系统不能运转”的故障级别，如果不能于12小时内解决故障，必须16小时内提出应急方案，确保业务系统的运行。故障解决后24小时内，提交故障处理报告，说明故障种类、故障原因、故障解决中使用的方法、故障损失、以及优化建议等情况。

3.3行为规范要求

1、项目实施人员将严格遵守我局的规章制度，严格按照相应的规章制度办事；

2、与采购人其他各合作方在协同工作时，将密切配合，同时会将双方协商的工作方案及时反馈到相关负责人员，再确定落实与否；

3、遵守保密原则。对服务过程中接触的系统中所有的信息和数据、服务过程中产生的信息和数据进行严格保密。不得以任何方式向第三方传递或泄漏任何相关信息或数据。

3.4服务工具要求

投标人在项目中用于安全检测使用的安全产品必须为厂商正版授权、符合国家安全标准及用户提出的有关质量标准的设备和产品。

3.5服务人员要求

1、中标人应成立针对我局安全服务的项目团队，人数要求不少于5人。其中项目经理1名，负责处理本项目有关事务（项目经理需具有持有PMP或信息系统项目管理师等相关技术资格证书）；机动安全专家1名，以便于在特殊情况下接替项目经理统筹安排项目工作（机动安全专家具有CISAW等相关技术资格证书）；安排1名专职安全工程师负责项目工作，必须具有较强的技术能力和项目沟通能力，持有CISP证书；在突发应急事件中能临时增加2名服务人员；

2、项目成员应严格遵守采购人的规章制度和保密制度,项目团队成员与中标公司均须与我局签定安全保密协议；

3、中标人应设立24小时热线电话，接受日常和应急安全服务要求和技术支持响应；

3.6项目验收要求

乙方根据项目服务合同，提供网络安全服务，项目实施完成后，将提供以下文档，配合完成项目验收工作。

1、提交最新修订版的《网络安全管理制度》；

2、提交《网络安全风险评估报告》、《信息安全风险评估应用层扫描报告》、《信息安全风险评估网络层扫描报告》；

3、提交《应急演练工作计划》、《应急演练工作方案》、《应急演练工作总结》文档；

4、提交信息安全培训计划、培训材料和视频；

5、提交网络安全联合检查工作文档汇编。

1. **评标定标方法**

本次采购采用综合评分法，是指投标文件满足招标文件全部资格性要求，且按照评审因素的量化指标评审得分最高的投标人为中标供应商的评标方法。

评标过程中，不得去掉报价中的最高报价和最低报价。

总得分（总分100分）=价格+技术部分+商务部分，分值及评分标准详见下表。

|  |  |  |  |
| --- | --- | --- | --- |
| 评分  因素 | 分值 | 评分内容 | 评分标准 |
| 报价  部分  （A） | 20分 | 报价得分  （20分） | 价格分满分为20分，以满足采购需求且报价最低的报价为评标基准价，其价格分为价格分满分，其他报价人的价格分统一按下列公式计算：  报价得分=（评标基准价/报价）×20。 |
| 技术部分  （B） | 45分 | B1、项目实施方案（25分） | 考察对项目工作内容的实施方案。建设内容包括但不限于：  ①项目实施总体思路；  ②实施本项目的主要人员配置；  ③质量保证措施；  ④技术方案；  ⑤人员管理制度。  提供材料包含以上任意一项得2分，最高得10分。在此基础上，根据各供应商的具体响应内容进一步评审，最高得15分。 |
| B2、项目重点难点分析、应对措施及相关的合理化建议（10分） | 考察根据采购文件的需求，制定贴切本项目的项目重点难点分析、应对措施及相关的合理化建议，根据各供应商的具体响应内容按照量化的评审因素指标进一步评审。  优评分标准：项目重点难点分析内容齐全，应对措施及相关的合理化建议清晰合理，得10分。  良评分标准：项目重点难点分析内容齐全，应对措施及相关的合理化建议较为清晰合理，得7分。  中评分标准：项目重点难点分析内容较为齐全，应对措施及相关的合理化建议一般，得4分。  差评分标准：内容不全的（没有完整包含项目重点、难点分析、应对措施及合理化建议等四部分）；应对措施及相关的合理化建议不清晰不合理的，得1分，如果没有提供具体内容的不得分。 |
|  | B3、质量保障措施及方案（10分） | 根据采购文件的需求，制定贴切本项目的质量（完成时间、安全）保障措施及方案以及项目完成（服务期满）后的服务承诺，根据各供应商的具体响应内容进行评审，最高得10分。 |
| 技术部分得分（B）=B1+B2+B3 | | |
| 商务部分（C） | 35分 | C1、投标人资质情况及通过相关认证情况（10分） | （一）评分内容：投标人资质情况及通过相关认证  以上累计最高得10分。  （二）评分依据：  （1）投标人具有中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质证书的，得2分；  （2）投标人具有国家信息安全漏洞库（CNNVD）技术支撑单位证书的，得2分；  （3）具有中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类），得2分  （4）具有中国信息安全测评中心颁发的安全服务资质证书（云计算安全类），得2分；  （5）具有中国网络安全审查技术与认证中心颁发的信息安全服务资质-安全开发服务证书的，得2分。  提供上述有效期内证明文件扫描件或复印件并加盖投标人公章。未按要求提供或提供不清晰导致专家无法判断的不得分。 |
| C2、同类项目业绩情况（8分） | 自2020年6月（以合同签订时间为准）至今，投标单位承接承担过为网络信息安全服务、渗透测试、安全检测等项目业绩，每提供一项业绩得2分，本项最高得分8分。  证明材料：中标通知书复印件或成交通知书复印件、合同关键页复印件。注：合同关键页应包括服务内容页、双方签字盖章页。 |
| C3、拟安排的项目团队情况（17分） | （一）评分内容：  为本项目拟安排项目团队成员：   1. 项目管理负责人（1名）：   （1）具备本科（或以上）学历，得1分  （2）具有具有 PMP 认证或人力资源和社会保障部门颁发的信息系统项目管理师证书的，得2分；  （3）具有信息系统安全认证专业人员CISSP 认证证书的，得2分；  2、技术服务团队人员不少于4名  （1）机动安全专家1名，特殊情况下接替项目管理负责人统筹安排项目工作，具有中国网络安全审查技术与认证中心颁发的CISAW证书，得2分；具有 PMP 认证或人力资源和社会保障部门颁发的信息系统项目管理师证书的证书，得2分；具有中国信息安全测评中心颁发的CISP认证得2分，最高得6分；  （2）在技术服务团队人员中每有1人具有中国信息安全测评中心颁发的CISP认证得2分，最高得6分；  以上资料均要求提供相关证书复印件、所有人员毕业证学信网查询记录截图及加盖投标人公章的近3个月的社保缴纳凭证作为证明材料。评分中出现无证明资料或未按要求提供或采购小组无法凭所提供资料判断是否得分的情况，一律作不得分处理。 |
| 商务部分得分（C）=C1+C2+C3 | |
| **评标总得分 Z=A+B+C** | | | |