政 府 采 购 合 同

（年 度 2021）

项目名称：国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目

（分标子项目）：

合同编号：GXJTZ[2021]110710(GX210517)

甲方(采购人名称)：国家税务总局广西壮族自治区税务局

乙方(供应商名称)：广西科奥信息技术有限公司

签 订 日 期：2021年 9月 28日

一、合同前文

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照采购文件规定采购方式、条款和成交供应商的承诺，甲乙双方经协商一致同意签订本合同。

1.合同文件

下列文件是构成本合同不可分割的部分：

(1)采购（项目）需求、招标（采购）文件规定的合同条款；

(2)报价表；

(3)投标文件技术部分和商务部分；

(4)甲、乙双方商定确认后的补充协议

(5)其他(根据实际情况需要增加的内容)。

2.合同标的(根据实际情况填写)

乙方应按照合同的规定，提供本项目采购文件中要求的服务（详见附件：服务内容一览表）。

3.服务时间、合同金额

本合同服务时间为签订合同之日起1年内完成等级保护和风险评估服务，合同单价为1,578,000.00元/年，合同总金额为人民币壹佰伍拾柒万捌仟元整(¥1,578,000.00)。本合同项下所有服务的全部税费均已包含于合同价中，甲方不再另行支付。

4.合同签订地

广西壮族自治区 南宁 市

5.合同生效

本合同一式六份，具有同等法律效力，甲方三份，乙方二份，采购代理机构一份（可根据需要另增加）。经甲乙双方法定代表人或其授权代表签字盖章，并在甲方收到乙方提交的履约保证金后生效。

甲方（盖章）：国家税务总局广西壮族自治区税务局　　法定代表人或其授权代表签字(或签章)：

乙方（盖章）：广西科奥信息技术有限公司　　法定代表人或其授权代表签字(或签章)：

二、合同前附表

序号	内容
1	合同名称：国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目 合同编号：GXJTZ[2021]110710(GX210517)
2	甲方名称：国家税务总局广西壮族自治区税务局
	甲方地址：广西壮族自治区南宁市青秀区园湖南路 26 号
	甲方联系人：何凡　电话：0771-5508053
	甲方开户银行名称：国家税务总局广西壮族自治区税务局 开户银行：交通银行股份有限公司南宁金源支行 银行账号：451060305010470003212
3	乙方名称：广西科奥信息技术有限公司
	乙方地址：南宁市青秀区双拥路 36-1 号绿城画卷 B 座 27 层 B2907 号房
	乙方联系人：莫胜坤　　电话：0771-5665929、18154597973
	乙方开户银行名称：中国工商银行股份有限公司南宁市琅东支行 账号：210 211 200 93003 22513
4	合同金额：人民币壹佰伍拾柒万捌仟元整(￥1,578,000.00)
5	服务时间、履行期：本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务年（月）或合同签订之日起_____个日历天内实施完毕，具体时间从_____年_____月_____日起至_____年月_____日止，即自合同生效之日起至合同全部权利义务履行完毕之日止。 合同期满，如甲方要求乙方继续提供本合同服务的，顺延至新的中标供应商提供服务之日或者甲方通知停止服务之日止。顺延期间，原合同服务内容、服务费用以及甲、乙双方的责任和义务等内容不变，但双方另有约定的除外。
6	服务地点：　广西南宁市民族大道国家税务总局广西壮族自治区税务局
7	验收方式及标准：按照采购需求、投标(响应)文件及国家、行业规定的技术标准及规范，双方到场共同验收。
8	付款方式：签订合同之日起 30 日内预付合同总金额的 50%；等级保护和风险评估服务完成后，甲方对项目进行验收，项目验收合格后 30 日内甲方向乙方支付合同剩余的 50%服务费，乙方在申请付款时将同等金额、合法有效的发票开具给甲方，否则甲方有权顺延付款。
9	履约保证金及其返还：本项目不要求乙方提供。
10	☑违约金约定：1.乙方违约或无正当理由造成解除合同的，按合同价款的 10%计算。逾期退回款项及违约金的，每逾期一天，按应退款项及违约金总额的 0.5%计算违约金。2.其它违约行为按违约服务款额 5%收取违约金。 ☑损失赔偿约定：按双方协商或经第三方评估的实际损失额进行赔偿。
11	误期赔偿费约定：如果乙方没有按照合同规定的时间交货和提供服务，甲方有权从货款或履约

	保证金中扣除误期赔偿费而不影响合同项下的其他补救方法。赔偿费按每日加收合同金额的0.5%计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的15%。
12	合同履行期限：自合同生效之日起至合同全部权利义务履行完毕之日止。
13	合同纠纷的解决方式： 首先通过双方协商解决，协商解决不成，则通过以下途径之一解决纠纷(请在方框内画“√”选择)： ☐ 提请_____仲裁委员会按照仲裁程序在_____(仲裁地)仲裁 ☑向人民法院提起诉讼

三、合同通用条款

1.定义

本合同下列术语应解释为：

1.1 “甲方”是指采购人。

1.2 “乙方”是指中标/成交供应商。

1.3 “合同”系指甲乙双方签署的、载明甲乙双方权利义务所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

1.4 “服务”是指乙方按照招标(采购)、投标(响应)文件要求，向采购人提供的技术支持服务。

1.5 “项目现场”是指甲方指定的最终服务地点。

1.6 “天”除非特别指出，“天”均为自然天。

2.服务标准

2.1 乙方为甲方交付的服务应符合招标（采购）文件和乙方的投标（响应）文件所述的内容，如果没有提及适用标准，则应符合相应的国家标准。这些标准必须是有关机构发布的最新版本的标准。

2.2 除非技术要求中另有规定，计量单位均采用中华人民共和国法定计量单位。

3.服务

3.1 乙方应按照合同的规定，提供下列服务甲方提供符合要求的服务。

4.知识产权

4.1 乙方应保证所提供的服务免受第三方提出侵犯其知识产权(专利权、商标权、版权等)的起诉。因侵害他人知识产权而产生的法律责任，全部由供应商承担。

4.2 甲方委托乙方开发的产品，甲方享有知识产权，未经甲方许可不得转让任何第三人。

5.保密条款

5.1 甲乙双方应对在本合同签订或履行过程中所接触的对方信息，包括但不限于知识产权、技术资料、技术诀窍、内部管理及其他相关信息，负有保密义务。

5.2 乙方在使用甲方为乙方及其工作人员提供的数据、程序、用户名、口令、资料及甲方相关的业务和技术文档，包括税收政策、方案设计细节、程序文件、数据结构，以及相关业务系统的硬软件、文档、测试和测试产生的数据时，应遵循以下规定：

(1)应以审慎态度避免泄露、公开或传播甲方的信息；

(2)未经甲方书面许可，不得对有关信息进行修改、补充、复制；

(3)未经甲方书面许可，不得将信息以任何方式(如E－mail)携带出甲方场所；

(4)未经甲方书面许可，不得将信息透露给任何其他人；

(5)甲方以书面形式提出的其他保密措施。

5.3 保密期限不受合同有效期的限制，在合同有效期结束后，信息接受方仍应承担保密义务，直至该

等信息成为公开信息。

5.4 甲乙双方如出现泄密行为，泄密方应承担相关的法律责任，包括但是不限于对由此给对方造成的经济损失进行赔偿。

5.5 乙方在本项目实施过程中发生违反网络安全规定行为，造成数据失窃或丢失、敏感信息泄露、主要业务系统瘫痪等不良后果的，自甲方或甲方主管机关做出认定之日起三年，税务系统各单位可以拒绝乙方参加税务系统政府采购活动。

6.服务质量保证

6.1 乙方应保证所提供的服务，符合合同规定的技术要求。如不符时，乙方应负全责并尽快处理解决，由此造成的损失和相关费用由乙方负责，甲方保留终止合同及索赔的权利。

6.2 乙方应保证通过执行合同中全部方案后，可以取得本合同规定的结果，达到本合同规定的预期目标。对任何情况下出现问题的，应尽快提出解决方案。

6.3 如果乙方提供的服务和解决方案不符合甲方要求，或在规定的时间内没有弥补缺陷，甲方有权采取一切必要的补救措施，由此产生的费用全部由乙方负责。

7.履约保证金

7.1 乙方应在签署合同前，以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式向甲方提供。

7.2 履约保证金具体金额及返还要求见合同条款前附表。

7.3 如乙方未能履行合同规定的义务，甲方有权按照本合同的约定从履约保证金中进行相应扣除。乙方应在甲方扣除履约保证金后 15 天内，及时补充扣除部分金额。

7.4 乙方不履行合同，或者履行合同义务不符合约定使得合同目的不能实现，履约保证金不予退还，给甲方造成的损失超过履约保证金数额的，还应当对超过部分予以赔偿。

8.服务时间、地点与验收

8.1 服务地点：合同条款前附表指定地点。

8.2 服务时间：合同条款前附表指定时间。

8.3 甲方应在乙方完成相关服务工作后及时对服务质量、技术指标、服务成果进行验收。

9.违约责任

9.1 服务缺陷的补救措施和索赔

(1)如果乙方提供的服务不符合本合同约定以及招标文件、投标文件关于服务的要求和承诺，乙方应按照甲方同意的下列一种或几种方式结合起来解决索赔事宜：

①乙方同意将服务款项目退还给甲方，由此发生的一切费用和损失由乙方承担。如甲方以适当的条件和方法购买与未履约标的相类似的服务，乙方应负担新购买类似服务所超出的费用。

②根据服务的质量状况以及甲方所遭受的损失，经过甲乙双方商定降低服务的价格。

(2)如果在甲方发出索赔通知后 10 日内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后 10 日内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付服务款中扣除索赔金额或者不退还履约保证金，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

9.2 迟延履约的违约责任

(1)乙方应按照本合同规定的时间、地点提供服务。

(2)在履行合同过程中，如果乙方遇到可能妨碍按时提供服务的情形时，应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延期提供服务。

(3)除甲乙双方另有约定外，如果乙方没有按照合同规定的时间提供服务，且没有在甲方同意的延长的期限内进行补救时，甲方有权从服务款、履约保证金中扣除或要求乙方另行支付误期赔偿费而不影响合同项下的其他补救方法。赔偿费按每日加收合同金额的 0.5%(各单位可根据实际情况重新设定)计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的 15%(各单位可根据实际情况重新设定)。

(4)如果乙方延迟履约超过 30 日，甲方有权终止全部或部分合同，并依其认为适当的条件和方法购买与未履约类似的服务，乙方应负担购买类似服务所超出的费用。但是，乙方应继续执行合同中未终止的部分。

9.3 未履行合同义务的违约责任

(1)守约方有权终止全部或部分合同。

(2)不予退还全额履约保证金。

(3)由违约一方支付违约金，违约金标准见合同条款前附表(各单位可根据实际情况自行约定)。

(4)违约金不足以弥补守约方实际损失、可预见或者应当预见的损失，由违约方全额予以赔偿。

10.不可抗力

10.1 如果合同双方因不可抗力而导致合同实施延误或合同无法实施，不应该承担误期赔偿或不能履行合同义务的责任。

10.2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

10.3 在不可抗力事件发生后，当事方应及时将不可抗力情况通知合同对方，在不可抗力事件结束后 3 日内以书面形式将不可抗力的情况和原因通知合同对方，并提供相应的证明文件。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行的协议。

11.合同纠纷的解决方式

11.1 合同各方应通过友好协商，解决在执行合同过程中所发生的或与合同有关的一切争端。如协商

30日内(根据实际情况设定)不能解决，可以按合同规定的方式提起仲裁或诉讼。

11.2 仲裁裁决应为最终裁决，对双方均具有约束力。

11.3 仲裁费除仲裁机关另有裁决外应由败诉方负担。

11.4 诉讼应由服务所在地人民法院管辖。诉讼费除人民法院另有判决外应由败诉方负担。

11.5 如仲裁或诉讼事项不影响合同其他部分的履行，则在仲裁或诉讼期间，除正在进行仲裁或诉讼的部分外，合同的其他部分应继续执行。

12.合同修改或变更

12.1 如无重大变故，甲方双方不得擅自变更合同。

12.2 如确需变更合同，甲乙双方应签署书面变更协议。变更协议为本合同不可分割的一部分。

12.3 在不改变合同其他条款的前提下，甲方有权在合同价款10%的范围内追加与合同标的相同的货物或服务，并就此与乙方签订补充合同，乙方不得拒绝。

13.合同中止

13.1 合同在履行过程中，因采购计划调整，甲方可以要求中止履行，待计划确定后继续履行；合同履行过程中因供应商就采购过程或结果提起投诉的，甲方认为有必要或财政部责令中止的，应当中止合同的履行。

14.违约终止合同

14.1 若出现如下情况，在甲方对乙方违约行为而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面通知书，提出终止部分或全部合同。

14.1.1 如果乙方未能在合同规定的期限或甲方同意延长的期限内提供服务；

14.1.2 因乙方技术人员自身技术能力、经验不足等原因造成甲方硬件设备、应用系统发生重大紧急故障或应用系统数据丢失，带来重大影响和损失的；

14.1.3 乙方对甲方硬件设备、应用系统重大紧急故障没有及时响应，或不能在规定时间内解决处理故障，恢复系统正常运行的；

14.1.4 不能满足本项目技术需求的管理要求和规范，且经多次（3次及以上）整改无明显改进，仍然不能满足要求的；

14.1.5 在合同规定的每个服务年度(12个自然月)内，在运行维护支持服务过程中，出现2次经甲乙双方确认的违规操作的。

14.2 如果甲方根据上述第14.1条的规定，终止了全部或部分合同，甲方可以适当的条件和方法购买乙方未能提供的服务，乙方应对甲方购买类似服务所超出的费用负责。同时，乙方应继续执行合同中未终止的部分。

15.破产终止合同

15.1 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。

15.2 该终止协议将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

16.其他情况的终止合同

16.1 若合同继续履行将给甲方造成重大损失的，甲方可以终止合同而不给予乙方任何补偿。

16.2 乙方在执行合同的过程中发生重大事故，对履行合同有直接影响的，甲方可以终止合同而不给予乙方任何补偿。

16.3 甲方因重大变故取消或部分取消原来的采购任务，导致合同全部或部分内容无须继续履行的，可以终止合同而不给予乙方任何补偿。

17.合同转让和分包

17.1 乙方不得以任何形式将合同转包，或部分或全部转让其应履行的合同义务。

17.2 除经甲方事先书面同意外，乙方不得以任何形式将合同分包。

18.适用法律

18.1 本合同适用中华人民共和国现行法律、行政法规和规章，如合同条款与法律、行政法规和规章不一致的，按照法律、行政法规和规章修改本合同。

19.合同语言

19.1 本合同语言为中文。

19.2 双方交换的与合同有关的信件和其他文件应用合同语言书写。

20.合同生效

20.1 本合同应在双方签字盖章和甲方收到乙方提供的履约保证金后生效。

21.合同效力

21.1 除本合同和甲乙双方书面签署的补充协议外，其他任何形式的双方约定和往来函件均不具有合同效力，对本项目无约束。

22.检查和审计

22.1 在本合同的履行过程中，甲方有权对乙方的合同履约情况进行阶段性检查，并对乙方投标（响应）时提供的相关资料进行复核。

22.2 在本合同的履行过程中，如果甲乙双方发生争议或者乙方没有按照合同约定履行义务，乙方应允许甲方检查乙方与实施本合同有关的账户和记录，并由甲方指定的审计人员对其进行审计。

四、合同补充条款（双方据实商定）

（无）

五、合同附件（与正件装订成册）

（一）服务内容一览表（乙方填制）；

（二）投标（响应）文件报价表部分（乙方提供）；

（三）投标（响应）文件技术部分和商务部分（乙方提供）；

（四）采购需求（与采购文件一致）；

（五）合同验收书格式（验收时填制，供参考）；

（六）政府采购项目履约保证金退付意见书（供参考）。

（一）服务内容一览表（乙方填制）

服务名称	单位	数量	金额（元）	具体服务承诺(包含但不限于服务内容、范围和基本要求)
等级保护测评服务	项	1	320000.00	提供针对本项目的技术、组织实施方案及售后服务方案。
风险评估服务	项	1	480000.00	提供针对本项目的技术、组织实施方案及售后服务方案。
安全检查服务	项	1	380000.00	提供针对本项目的技术、组织实施方案及售后服务方案。
源代码检测服务	项	1	300000.00	提供针对本项目的技术、组织实施方案及售后服务方案。
密码测评	项	1	98000.00	提供针对本项目的技术、组织实施方案及售后服务方案。
总计			大写:人民币 壹佰伍拾柒万捌仟 元 小写:¥1578000.00	

（二）投标（响应）文件报价表部分（乙方提供）

一、资格和报价部分

（一）投标函

投 标 函

致国家税务总局广西壮族自治区税务局(采购人或采购代理机构)：

根据国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目(项目名称)(项目编号：GXJTZ[2021]110710（GX210517）)的投标邀请，莫胜坤、测评工程师 (姓名、职务)代表投标人广西科奥信息技术有限公司、南宁市青秀区双拥路36-1号绿城画卷B座27层B2907号房(投标人名称、地址)参加本项目招标的有关活动。据此函，作如下承诺：

1. 同意在本项目招标文件中规定的开标日起90天遵守本投标文件中的承诺，且在期满之前均具有约束力。

2. 具备政府采购相关法律法规规定的参加政府采购活动的供应商应当具备的条件：

(1)具有独立承担民事责任的能力；

(2)具有良好的商业信誉和健全的财务会计制度；

(3)具有履行合同所必需的设备和专业技术能力；

(4)有依法缴纳税收和社会保障资金的良好记录；

(5)参加此项采购活动前3年内，在经营活动中没有重大违法记录。

3. 具备本项目招标文件中规定的其他资格条件。

4. 提供投标人须知规定的全部投标文件，包括投标文件正本壹份，副本肆份，电子文档壹份，开标一览表(投标报价表、投标保证金)壹份。

5. 已详细审阅全部招标文件(包括招标文件澄清函)，理解投标人须知的所有条款。

6. 完全理解贵方“最低报价不能作为中标的保证”的规定。

7. 接受招标文件中全部合同条款，且无任何异议；保证忠实

地执行双方所签订的合同，并承担合同规定的责任和义务。

8. 完全满足和响应招标文件中的各项商务和技术要求，若有偏差，已在投标文件中明确说明。

9. 如果在开标后规定的投标有效期内撤回投标，贵方可不予退还我方的投标保证金。

10. 愿意提供任何与投标有关的数据、情况和技术资料等。

11. 我方已详细审核全部投标文件、参考资料及有关附件，确认无误。

12. 对本次招标内容及与本项目有关的知识产权、技术资料、商业秘密及相关信息保密。

13. 与采购人和采购代理机构无任何的隶属关系或者其他利害关系。

附件 1—1：法定代表人（负责人）身份证复印件（法定代表人参加投标）

附件 1—2：法定代表人（负责人）授权书（授权代表参加投标）

附件 1—3：授权委托书（自然人提供）

投标人名称：广西科奥信息技术有限公司投标人公章：_____

投标人地址：南宁市青秀区双拥路 36-1 号绿城画卷 B 座 27 层 B2907 号房

邮编：530022

电话：0771-5665929 传真：0771-5665929

法定代表人（负责人）或投标人代表（签字或盖章）：莫胜伸

联系电话：18154597973

日期：2021 年 9 月 23 日

（二）开标一览表

开标一览表

（服务类项目适用）

序号	项目名称	国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目	项目编号	GXJTZ[2021]110710（GX210517）
1	包号	/		
2	报价	大写：人民币 壹佰伍拾柒万捌仟 元 小写：¥ 1578000.00000		
3	服务时间	本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务。		
	…			
	备注			

说明：

1. 所有价格均用人民币表示，单位为元，精确到小数点后五位数。

2. 此表的总报价是所有需采购方支付的本次采购标的金额总数，即投标总价。投标总价须包含完成用户需求要求所有内容的全部费用。

投标人名称（公章）：广西科奥信息技术有限公司

法定代表人或其授权代表签字：黄旭伸

日期：2021 年 9 月 23 日

（三）分项价格表

分项价格表

（服务类项目适用）

项目名称：国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目

项目编号：GXJTZ[2021]110710（GX210517）

包号：/　　金额单位：元

序号	服务内容	报价	备注 （收费依据、收费标准等）
1	等级保护测评服务	320000.00000	/
2	风险评估服务	480000.00000	/
3	安全检查服务	380000.00000	/
4	源代码检测服务	300000.00000	/
5	密码测评	98000.00000	/
总计		大写：人民币 壹佰伍拾柒万捌仟 元 小写：¥ 1578000.00000	

1. 如本表格不适合投标单位的实际情况，可根据本表格式自行制表填写。
2. 投标报价包含实施和完成本项目需求要求所有内容的全部费用，此表报价应与“开标一览表”投标报价相一致。
3. 所有价格均用人民币表示，单位为元，精确到小数点后五位数。

供应商（公章）：广西科奥信息技术有限公司

法定代表人或其授权代表（签字或盖章）：

日期：2021年 9 月 23 日

二、技术响应与偏离表

技术响应与偏离表

项目名称：国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目

项目编号：GXITZ[2021]110710（GX210517）

包号：/

品目号	货物或服务名称	招标规格	技术指标要求	投标响应情况	偏离	说明
1	等级保护测评服务	对国家税务总局广西自治区税务局的8个信息系统开展等级保护测评工作； 1、测评依据 (1)《安全保护等级划分准则》（GB17859-1999） (2)《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2018） (3)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019） 2、测评内容：	对国家税务总局广西自治区税务局的8个信息系统开展等级保护测评工作； 1、测评依据 (1)《安全保护等级划分准则》（GB17859-1999） (2)《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2018） (3)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019） 2、测评内容：	**我公司承诺按以下要求响应：** 对国家税务总局广西自治区税务局的8个信息系统开展等级保护测评工作； 1、测评依据 (1)《安全保护等级划分准则》（GB17859-1999） (2)《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2018） (3)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）	无偏离	/

		须按照信息系统等级保护测评规范，制定详实的测评方案；在保证测评质量的前提下，按时完成测评工作，并提交测评报告；根据所测系统的测评报告，提供切实可行的整改技术方案，并协助用户按照技术方案做好所测系统的安全整改工作，直至消除安全隐患。 测评应包括以下内容： （1）物理安全评估：应包括机房环境和硬件设施物理安全等内容； （2）网络安全测评：应包括网络结构、网络设备及网络安全设备等内容； （3）主机安全测评：应包括操作系统及数据库系统等内容； （4）应用安全测评：应包括系统应用的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护等内容； （5）数据安全及备份恢复测评：应包括系统数据完整性、数据保密性、备份和恢复等内容；	须按照信息系统等级保护测评规范，制定详实的测评方案：在保证测评质量的前提下，按时完成测评工作，并提交测评报告；根据所测系统的测评报告，提供切实可行的整改技术方案，并协助用户按照技术方案做好所测系统的安全整改工作，直至消除安全隐患。 测评应包括以下内容： （1）物理安全评估：应包括机房环境和硬件设施物理安全等内容； （2）网络安全测评：应包括网络结构、网络设备及网络安全设备等内容； （3）主机安全测评：应包括操作系统及数据库系统等内容； （4）应用安全测评：应包括系统应用的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护等内容； （5）数据安全及备份恢复测评：应包括系统数据完整性、数据保密性、备份和恢复等内容； （6）安全管理制度评估：应包括	2、测评内容： 须按照信息系统等级保护测评规范，制定详实的测评方案；在保证测评质量的前提下，按时完成测评工作，并提交测评报告；根据所测系统的测评报告，提供切实可行的整改技术方案，并协助用户按照技术方案做好所测系统的安全整改工作，直至消除安全隐患。 测评应包括以下内容： （1）物理安全评估：应包括机房环境和硬件设施物理安全等内容； （2）网络安全测评：应包括网络结构、网络设备及网络安全设备等内容； （3）主机安全测评：应包括操作系统及数据库系统等内容； （4）应用安全测评：应包括系统应用的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护等内容； （5）数据安全及备份恢复测评：应包括系统数据完整性、数据保密性、备份和恢复等内容；		

		（6）安全管理制度评估：应包括管理制度、制定和发布、评审和修订等内容； （7）安全管理机构评估：应包括岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等内容； （8）人员安全管理评估：应包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容； （9）建设管理评估：应包括系统建设的全过程，系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等内容； （10）运维管理评估：应包括资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。 3、测评方法 在安全测评过程中，应采用访谈、检查、测试、工具扫描等	管理制度、制定和发布、评审和修订等内容； （7）安全管理机构评估：应包括岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等内容； （8）人员安全管理评估：应包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容； （9）建设管理评估：应包括系统建设的全过程，系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等内容； （10）运维管理评估：应包括资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。 3、测评方法 在安全测评过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求	（6）安全管理制度评估：应包括管理制度、制定和发布、评审和修订等内容； （7）安全管理机构评估：应包括岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等内容； （8）人员安全管理评估：应包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容； （9）建设管理评估：应包括系统建设的全过程，系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等内容； （10）运维管理评估：应包括资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。 3、测评方法 在安全测评过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段		

		国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。在招标文件中详细描述所采用的测评方法。 对信息系统进行安全漏洞检测和挖掘，检测例如缓冲区溢出、SQL 注入和跨站脚本等常见安全漏洞，并提供漏洞修补建议及时采取适当的处理措施进行修补，有效阻止安全隐患被利用和发生安全事件。	相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。在招标文件中详细描述所采用的测评方法。 对信息系统进行安全漏洞检测和挖掘，检测例如缓冲区溢出、SQL 注入和跨站脚本等常见安全漏洞，并提供漏洞修补建议及时采取适当的处理措施进行修补，有效阻止安全隐患被利用和发生安全事件。	进行，并与国家相关规范及标准的要求相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。在招标文件中详细描述所采用的测评方法。 对信息系统进行安全漏洞检测和挖掘，检测例如缓冲区溢出、SQL 注入和跨站脚本等常见安全漏洞，并提供漏洞修补建议及时采取适当的处理措施进行修补，有效阻止安全隐患被利用和发生安全事件。		
2	风险评估服务	对国家税务总局广西壮族自治区税务局 12 个重要信息系统进行风险评估，对信息系统的资产、威胁、脆弱性进行识别分析，并对现有的管理制度和技术措施进行安全评估，提高重要信息系统防范风险的能力。供应商所出具的报告需具备产品质量评价、成果及司法鉴定，具有法律效力。 1、评估目标 （1）对现有的信息安全管理制	对国家税务总局广西壮族自治区税务局 12 个重要信息系统进行风险评估，对信息系统的资产、威胁、脆弱性进行识别分析，并对现有的管理制度和技术措施进行安全评估，提高重要信息系统防范风险的能力。供应商所出具的报告需具备产品质量评价、成果及司法鉴定，具有法律效力。 1、评估目标 （1）对现有的信息安全管理制度和技术措施的有效性进行风险评	**我公司承诺按以下要求响应：** 对国家税务总局广西壮族自治区税务局 12 个重要信息系统进行风险评估，对信息系统的资产、威胁、脆弱性进行识别分析，并对现有的管理制度和技术措施进行安全评估，提高重要信息系统防范风险的能力。供应商所出具的报告需具备产品质量评价、成果及司法鉴定，具有法律效力。 1、评估目标	无偏离	/

		度和技术措施的有效性进行风险评估。 （2）对系统资产、威胁、脆弱性进行识别、分析。 （3）提出安全整改建议。 2、评估范围 包括：系统所涉及的物理环境、网络、主机、系统软件、应用软件、管理制度、人员等。 3、评估内容 （1）信息系统安全管理状况检查 评估各种安全制度的建立情况。包括：终端计算机访问互联网的相关制度；终端计算机接入内网的相关制度；使用移动存储介质的制度；系统业务应用人员、系统的开发、维护、管理人员、维护人员相关的安全管理制度等。 （2）网络结构、网络安全设备评估范围包括：分析网络拓扑结构是否清晰划分网络边界；评估网络的访问控制措施。 （3）对资产的脆弱性进行收集和整理	估。 （2）对系统资产、威胁、脆弱性进行识别、分析。 （3）提出安全整改建议。 2、评估范围 包括：系统所涉及的物理环境、网络、主机、系统软件、应用软件、管理制度、人员等。 3、评估内容 （1）信息系统安全管理状况检查评估各种安全制度的建立情况。包括：终端计算机访问互联网的相关制度；终端计算机接入内网的相关制度；使用移动存储介质的制度；系统业务应用人员、系统的开发、维护、管理人员、维护人员相关的安全管理制度等。 （2）网络结构、网络安全设备评估范围包括：分析网络拓扑结构是否清晰划分网络边界；评估网络的访问控制措施。 （3）对资产的脆弱性进行收集和整理 物理环境，包括机房环境，空调，防雷接地等； 检查交换机，路由器的口令设置	（1）对现有的信息安全管理制度和技术措施的有效性进行风险评估。 （2）对系统资产、威胁、脆弱性进行识别、分析。 （3）提出安全整改建议。 2、评估范围 包括：系统所涉及的物理环境、网络、主机、系统软件、应用软件、管理制度、人员等。 3、评估内容 （1）信息系统安全管理状况检查 评估各种安全制度的建立情况。包括：终端计算机访问互联网的相关制度；终端计算机接入内网的相关制度；使用移动存储介质的制度；系统业务应用人员、系统的开发、维护、管理人员、维护人员相关的安全管理制度等。 （2）网络结构、网络安全设备评估范围包括：分析网络拓扑结构是否清晰划分网络边界；评估网络的访问控制措施。 （3）对资产的脆弱性进行收集和整理		

		物理环境，包括机房环境，空调、防雷接地等； 检查交换机，路由器的口令设置和管理，配置文件的备份等； 检查路由器操作系统是否存在安全漏洞；检查端口开放、管理员口令设置和管理、访问控制表；关键路由设备是否有冗余配置等。 防火墙、入侵检测系统、防病毒、桌面管理、审计等，评估安全配置的有效性。 服务器：用户口令、共享资源、系统服务安全、系统安全补丁、日志记录审计、木马检测等。 （4）应用系统 评估应用系统。 数据库：数据库系统及应用数据 操作系统：应用系统和数据库涉及到的主机操作系统。 (5) 灾难备份情况 根据信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络	和管理，配置文件的备份等； 检查路由器操作系统是否存在安全漏洞；检查端口开放、管理员口令设置和管理、访问控制表；关键路由设备是否有冗余配置等。 防火墙、入侵检测系统、防病毒、桌面管理、审计等，评估安全配置的有效性。 服务器：用户口令、共享资源、系统服务安全、系统安全补丁、日志记录审计、木马检测等。 （4）应用系统 评估应用系统。 数据库：数据库系统及应用数据 操作系统：应用系统和数据库涉及到的主机操作系统。 (5) 灾难备份情况 根据信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、 数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。 4、评估依据	物理环境，包括机房环境，空调，防雷接地等； 检查交换机，路由器的口令设置和管理，配置文件的备份等； 检查路由器操作系统是否存在安全漏洞；检查端口开放、管理员口令设置和管理、访问控制表；关键路由设备是否有冗余配置等。 防火墙、入侵检测系统、防病毒、桌面管理、审计等，评估安全配置的有效性。 服务器：用户口令、共享资源、系统服务安全、系统安全补丁、日志记录审计、木马检测等。 （4）应用系统 评估应用系统。 数据库：数据库系统及应用数据操作系统：应用系统和数据库涉及到的主机操作系统。 (5) 灾难备份情况 根据信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管		

		系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。 4、评估依据 （1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GB/T 20984-2007（信息安全技术 信息安全风险评估规范） （4）GB_T31509-2015 （信息安全技术 信息安全风险评估实施指南） （5）GB/T9361-2011 计算机场地安全要求 （6）GB17859-1999 计算机信息系统安全保护等级划分准则 （7）GB/T 18336.3-2008 信息安全技术 信息技术安全性评估准则 （8）GB/T 22081-2008 信息技术 信息安全管理实用规则 （9）行业主管部门对业务系统的要求和制度 （10）系统相关单位的安全要求	（1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GB/T 20984-2007（信息安全技术 信息安全风险评估规范） （4）GB_T31509-2015 （信息安全技术 信息安全风险评估实施指南） （5）GB/T9361-2011 计算机场地安全要求 （6）GB17859-1999 计算机信息系统安全保护等级划分准则 （7）GB/T 18336.3-2008 信息安全技术 信息技术安全性评估准则 （8）GB/T 22081-2008 信息技术 信息安全管理实用规则 （9）行业主管部门对业务系统的要求和制度 （10）系统相关单位的安全要求 （11）系统本身的实时性或性能要求	理能力、技术支持能力等七大要素。 4、评估依据 （1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GB/T 20984-2007（信息安全技术 信息安全风险评估规范） （4）GB_T31509-2015 （信息安全技术 信息安全风险评估实施指南） （5）GB/T9361-2011 计算机场地安全要求 （6）GB17859-1999 计算机信息系统安全保护等级划分准则 （7）GB/T 18336.3-2008 信息安全技术 信息技术安全性评估准则 （8）GB/T 22081-2008 信息技术 信息安全管理实用规则 （9）行业主管部门对业务系统的要求和制度 （10）系统相关单位的安全要求 （11）系统本身的实时性或性能要求		

		（11）系统本身的实时性或性能要求				
3	安全检查服务	对国家税务总局广西壮族自治区税务局、各市税务局和各稽查局等 19 个单位进行安全检查，检查各单位的网络安全管理情况、安全技术防护情况、应急工作开展情况、等级保护工作落实情况、绩效相关安全工作落实情况等，指导各单位进一步健全和完善网络安全工作。 1、项目要求 通过开展信息安全检查，以查促建、以查促管、以查促改、以查促防，增强安全意识，落实安全责任，深入分析安全风险，系统评估安全状况，全面排查安全隐患，进一步健全安全管理制度，完善安全防护措施，提升自主可控水平和安全防护能力，预防和减少信息安全事件的发生，切实保障重要信息与信息系统的安全稳定运行。 2、检查依据	对国家税务总局广西壮族自治区税务局、各市税务局和各稽查局等 19 个单位进行安全检查，检查各单位的网络安全管理情况、安全技术防护情况、应急工作开展情况、等级保护工作落实情况、绩效相关安全工作落实情况等，指导各单位进一步健全和完善网络安全工作。 1、项目要求 通过开展信息安全检查，以查促建、以查促管、以查促改、以查促防，增强安全意识，落实安全责任，深入分析安全风险，系统评估安全状况，全面排查安全隐患，进一步健全安全管理制度，完善安全防护措施，提升自主可控水平和安全防护能力，预防和减少信息安全事件的发生，切实保障重要信息与信息系统的安全稳定运行。 2、检查依据 (1)《国家信息化领导小组关于加强信息安全保障工作的意见》(中	**我公司承诺按以下要求响应：** 对国家税务总局广西壮族自治区税务局、各市税务局和各稽查局等 19 个单位进行安全检查，检查各单位的网络安全管理情况、安全技术防护情况、应急工作开展情况、等级保护工作落实情况、绩效相关安全工作落实情况等，指导各单位进一步健全和完善网络安全工作。 1、项目要求 通过开展信息安全检查，以查促建、以查促管、以查促改、以查促防，增强安全意识，落实安全责任，深入分析安全风险，系统评估安全状况，全面排查安全隐患，进一步健全安全管理制度，完善安全防护措施，提升自主可控水平和安全防护能力，预防和减少信息安全事件的发生，切实保障重要信息与信息系统的安全稳定运行。 2、检查依据	无偏离	/

		(1)《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号) (2)《国务院办公厅关于印发<政府信息系统安全检查办法>的通知》(国办发[2009]28 号) (3)《广西壮族自治区人民政府办公厅关于做好全区政府信息系统年度安全检查工作的通知》(桂政办发[2010]145 号) (4)《GM/T 0054-2018 信息系统密码应用基本要求》 3、信息安全检查内容 根据工作需要重点抽查但不限于以下内容: (1)信息安全管理情况 按照国家信息安全政策和标准规范要求,建立健全信息安全管理制度及落实情况。重点检查单位信息安全主管领导、管理机构和工作人员履职情况,信息安全责任制落实及事故责任追究情况,人员、资产、采购、外包服务等日常安全管理情况,信息安全规划制定情况,信息安全从业人员情况,信息	办发[2003]27 号) (2)《国务院办公厅关于印发<政府信息系统安全检查办法>的通知》(国办发[2009]28 号) (3)《广西壮族自治区人民政府办公厅关于做好全区政府信息系统年度安全检查工作的通知》(桂政办发[2010]145 号) (4)《GM/T 0054-2018 信息系统密码应用基本要求》 3、信息安全检查内容 根据工作需要重点抽查但不限于以下内容: (1)信息安全管理情况 按照国家信息安全政策和标准规范要求,建立健全信息安全管理制度及落实情况。重点检查单位信息安全主管领导、管理机构和工作人员履职情况,信息安全责任制落实及事故责任追究情况,人员、资产、采购、外包服务等日常安全管理情况,信息安全规划制定情况,信息安全从业人员情况,信息安全经费保障情况等。 (2)技术防护情况 按照国家信息安全政策和标准规	(1)《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号) (2)《国务院办公厅关于印发<政府信息系统安全检查办法>的通知》(国办发[2009]28 号) (3)《广西壮族自治区人民政府办公厅关于做好全区政府信息系统年度安全检查工作的通知》(桂政办发 2010]145 号) (4)《GM/T 0054-2018 信息系统密码应用基本要求》 3、信息安全检查内容 根据工作需要重点抽查但不限于以下内容: (1)信息安全管理情况 按照国家信息安全政策和标准规范要求,建立健全信息安全管理制度及落实情况。重点检查单位信息安全主管领导、管理机构和工作人员履职情况,信息安全责任制落实及事故责任追究情况,人员、资产、采购、外包服务等日常安全管理情况,信息安全规划制定情况,信息安全从业人员情况,信息安全经费保障情		

		安全经费保障情况等。 （2）技术防护情况 按照国家信息安全政策和标准规范要求，建立健全技术防护体系及安全防护情况。重点检查防病毒、防攻击、防篡改、防瘫痪、防泄密措施及有效性；信息边界防护措施，互联网接入安全措施，无线信息安全防护策略；服务器、信息设备、安全设备等安全策略配置，应用系统安全功能及有效性；终端计算机、移动存储介质安全防护措施；重要数据传输、存储的安全防护措施；重要信息安全漏洞修复情况等。 (3)应急工作情况 按照国家信息与信息安全事件应急预案要求，建立健全信息安全应急工作体系情况。重点检查信息安全事件应急预案制修订情况、应急演练情况；应急技术支撑队伍、灾难备份措施建设情况；重大信息安全事件处置情况等。 (4)灾难备份情况	范要求，建立健全技术防护体系及安全防护情况。重点检查防病毒、防攻击、防篡改、防瘫痪、防泄密措施及有效性；信息边界防护措施，互联网接入安全措施，无线信息安全防护策略；服务器、信息设备、安全设备等安全策略配置，应用系统安全功能及有效性；终端计算机、移动存储介质安全防护措施；重要数据传输、存储的安全防护措施；重要信息安全漏洞修复情况等。 (3)应急工作情况 按照国家信息与信息安全事件应急预案要求，建立健全信息安全应急工作体系情况。重点检查信息安全事件应急预案制修订情况、应急演练情况；应急技术支撑队伍、灾难备份措施建设情况；重大信息安全事件处置情况等。 (4)灾难备份情况 针对信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能	况等。 （2）技术防护情况 按照国家信息安全政策和标准规范要求，建立健全技术防护体系及安全防护情况。重点检查防病毒、防攻击、防篡改、防瘫痪、防泄密措施及有效性；信息边界防护措施，互联网接入安全措施，无线信息安全防护策略；服务器、信息设备、安全设备等安全策略配置，应用系统安全功能及有效性；终端计算机、移动存储介质安全防护措施；重要数据传输、存储的安全防护措施；重要信息安全漏洞修复情况等。 (3)应急工作情况 按照国家信息与信息安全事件应急预案要求，建立健全信息安全应急工作体系情况。重点检查信息安全事件应急预案制修订情况、应急演练情况；应急技术支撑队伍、灾难备份措施建设情况；重大信息安全事件处置情况等。 (4)灾难备份情况 针对信息化项目建设时设计的		

		针对信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。 (5)宣传教育培训情况 重点检查信息安全宣传教育、领导干部及各级人员信息安全基础培训、信息安全人员专业技术培训等情况。 (6)等级保护工作落实情况按照国家信息安全等级保护工作标准规范和法规的要求，重点检查重要信息系统定级备案、安全测评和安全建设整改等等级保护制度落实情况。 (7)商用密码使用情况 按照国家商用密码管理标准规范和法规的要求，重点检查重要信息和信息系统中密码技术、产品和服务的使用情况。重点是信息设备中采用密码技术的情况；各类密码产品的使用情况，及其安全策略配置情	力、技术支持能力等七大要素。 (5)宣传教育培训情况 重点检查信息安全宣传教育、领导干部及各级人员信息安全基础培训、信息安全人员专业技术培训等情况。 (6)等级保护工作落实情况按照国家信息安全等级保护工作标准规范和法规的要求，重点检查重要信息系统定级备案、安全测评和安全建设整改等等级保护制度落实情况。 (7)商用密码使用情况 按照国家商用密码管理标准规范和法规的要求，重点检查重要信息和信息系统中密码技术、产品和服务的使用情况。重点是信息设备中采用密码技术的情况；各类密码产品的使用情况，及其安全策略配置情况；密码应用集成商、运营商的基本情况；各重要信息与信息系统开展密码测评情况等。 (8)安全问题整改情况 上一年度各类信息安全检查所发现问题的整改情况及整改效果。	灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。 (5)宣传教育培训情况 重点检查信息安全宣传教育、领导干部及各级人员信息安全基础培训、信息安全人员专业技术培训等情况。 (6)等级保护工作落实情况 按照国家信息安全等级保护工作标准规范和法规的要求，重点检查重要信息系统定级备案、安全测评和安全建设整改等等级保护制度落实情况。 (7)商用密码使用情况 按照国家商用密码管理标准规范和法规的要求，重点检查重要信息和信息系统中密码技术、产品和服务的使用情况。重点是信息设备中采用密码技术的情况；各类密码产品的使用情况，及其安全策略配置情况；密码应用集成商、运营商的基本情况；各重		

		况、密码应用集成商、运营商的基本情况；各重要信息与信息系统开展密码测评情况等。 (8) 安全问题整改情况 上一年度各类信息安全检查所发现问题的整改情况及整改效果		要信息与信息系统开展密码测评情况等。 (8) 安全问题整改情况 上一年度各类信息安全检查所发现问题的整改情况及整改效果。		
4	源代码检测服务	对国家税务总局广西壮族自治区税务局 8 个应用系统进行应用系统源代码审计，形成源代码安全审计报告和安全功能测评报告，经评审后形成安全开发评审报告。 1、检测依据 安全检测主要依据以下标准： （1）《ISO9126 软件产品评价—质量特性及其使用指南》 （2）《GB/T 20271-2006 信息安全技术信息系统安全通用技术要求》 （3）《GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求》 （4）《ISO9126 软件产品评价—质量特性及其使用指南》 （5）《GB/T 28452-2012 信息	对国家税务总局广西壮族自治区税务局 8 个应用系统进行应用系统源代码审计，形成源代码安全审计报告和安全功能测评报告，经评审后形成安全开发评审报告。 1、检测依据 安全检测主要依据以下标准： （1）《ISO9126 软件产品评价—质量特性及其使用指南》 （2）《GB/T 20271-2006 信息安全技术信息系统安全通用技术要求》 （3）《GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求》 （4）《ISO9126 软件产品评价—质量特性及其使用指南》 （5）《GB/T 28452-2012 信息安	**我公司承诺按以下要求响应：** 对国家税务总局广西壮族自治区税务局 8 个应用系统进行应用系统源代码审计，形成源代码安全审计报告和安全功能测评报告，经评审后形成安全开发评审报告。 1、检测依据 安全检测主要依据以下标准： （1）《ISO9126 软件产品评价—质量特性及其使用指南》 （2）《GB/T 20271-2006 信息安全技术信息系统安全通用技术要求》 （3）《GB/T 20273-2006 信息安全技术数据库管理系统安全技术要求》 （4）《ISO9126 软件产品评价	无偏离	/

		安全技术应用软件系统通用安全技术要求》 （6）《GBT 20988-2007 信息安全技术信息系统灾难恢复规范》 （7）《GB/T 28458-2020 信息安全技术网络安全漏洞标识与描述规范》 （8）《GB/T 30279-2020 信息安全技术网络安全漏洞分类分级指南》 （9）CVE(Common Vulnerabilities & Exposures)公共漏洞字典表 （10）OWASP 十大 Web 漏洞（Open Web Application Security Project） 本项目相关文档，包括开发实施合同、需求规格说明书、系统详细设计、部署安装详细说明说、操作手册和功能列表等 2、检测分析 （1） 静态安全性测试分析 要求采用先进的源代码审计工具对源代码进行完整的自动化审计工作，并得出结果报告，	全技术应用软件系统通用安全技术要求》 （6）《GBT 20988-2007 信息安全技术信息系统灾难恢复规范》 （7）《GB/T 28458-2020 信息安全技术网络安全漏洞标识与描述规范》 （8）《GB/T 30279-2020 信息安全技术网络安全漏洞分类分级指南》 （9）CVE(Common Vulnerabilities & Exposures)公共漏洞字典表 （10）OWASP 十大 Web 漏洞（Open Web Application Security Project） 本项目相关文档，包括开发实施合同、需求规格说明书、系统详细设计、部署安装详细说明说、操作手册和功能列表等 2、检测分析 （1） 静态安全性测试分析 要求采用先进的源代码审计工具对源代码进行完整的自动化审计工作，并得出 结果报告，再由专业检测人员进	一质量特性及其使用指南》 （5）《GB/T 28452-2012 信息安全技术应用软件系统通用安全技术要求》 （6）《GBT 20988-2007 信息安全技术信息系统灾难恢复规范》 （7）《GB/T 28458-2020 信息安全技术网络安全漏洞标识与描述规范》 （8）《GB/T 30279-2020 信息安全技术网络安全漏洞分类分级指南》 （9）CVE(Common Vulnerabilities & Exposures)公共漏洞字典表 （10）OWASP 十大 Web 漏洞（Open Web Application Security Project） 本项目相关文档，包括开发实施合同、需求规格说明书、系统详细设计、部署安装详细说明说、操作手册和功能列表等 2、检测分析 （1） 静态安全性测试分析 要求采用先进的源代码审计工具对源代码进行完整的自动化		

		再由专业检测人员进行人工判断、分析，最终获得较为准确的软件代码安全问题结果。 源代码审计的内容包括： 1）前后台分离的运行架构 2）WEB 服务的目录权限分类 3）认证会话与应用平台的结合 4）数据库的配置规范 5）SQL 语句的编写规范 6）WEB 服务的权限配置 7）对抗爬虫引擎的处理措施 （2） 人工审查 使用自带审查功能对源代码漏洞进行人工审查，分析排除源代码漏洞中的误报内容，同时检查真实存在漏洞代码的关联点，查看是否有漏报，分析排查后将结果生成报告并导出，作为正式报告编写的参考内容。	行人工判断、分析，最终获得较为准确的软件代码安全问题结果。 源代码审计的内容包括： 1）前后台分离的运行架构 2）WEB 服务的目录权限分类 3）认证会话与应用平台的结合 4）数据库的配置规范 5）SQL 语句的编写规范 6）WEB 服务的权限配置 7）对抗爬虫引擎的处理措施 （2） 人工审查 使用自带审查功能对源代码漏洞进行人工审查，分析排除源代码漏洞中的误报内容，同时检查真实存在漏洞代码的关联点，查看是否有漏报，分析排查后将结果生成报告并导出，作为正式报告编写的参考内容。	审计工作，并得出结果报告，再由专业检测人员进行人工判断、分析，最终获得较为准确的软件代码安全问题结果。 源代码审计的内容包括： 1）前后台分离的运行架构 2）WEB 服务的目录权限分类 3）认证会话与应用平台的结合 4）数据库的配置规范 5）SQL 语句的编写规范 6）WEB 服务的权限配置 7）对抗爬虫引擎的处理措施 （2） 人工审查 使用自带审查功能对源代码漏洞进行人工审查，分析排除源代码漏洞中的误报内容，同时检查真实存在漏洞代码的关联点，查看是否有漏报，分析排查后将结果生成报告并导出，作为正式报告编写的参考内容。		
5	密码测评	对 1 个信息系统进行商用密码应用安全性评估工作，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到《GM/T0054-2018 信息系统密	对 1 个信息系统进行商用密码应用安全性评估工作，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到《GM/T0054-2018 信息系统密码	**我公司承诺按以下要求响应：** 对 1 个信息系统进行商用密码应用安全性评估工作，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，	无偏离	/

		码应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。 1、检测依据 （1）《商用密码应用安全性评估管理办法（试行）》 （2）《信息系统密码测评要求（试行）》 （3）《商用密码应用安全性评估测评过程指南（试行）》 （4）《商用密码应用安全性评估测评作业指导书（试行）》 （5）《商用密码应用安全性评估测评工具使用需求说明（试行）》 （6）《GM/T0054-2018 信息系统密码应用基本要求》 2、检测内容及分析 主要检测内容包括： （1） 物理和环境安全测评 包括：身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性等测评内容； （2） 网络和通信安全测评 包括：身份鉴别、通信数据完整性、通信过程中重要数据的	应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。 1、检测依据 （1）《商用密码应用安全性评估管理办法（试行）》 （2） 《信息系统密码测评要求（试行）》 （3）《商用密码应用安全性评估测评过程指南（试行）》 （4）《商用密码应用安全性评估测评作业指导书（试行）》 （5）《商用密码应用安全性评估测评工具使用需求说明（试行）》 （6）《GM/T0054-2018 信息系统密码应用基本要求》 2、检测内容及分析 主要检测内容包括： （1） 物理和环境安全测评 包括：身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性等测评内容； （2） 网络和通信安全测评 包括：身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完	以确保被测信息系统达到《GM/T0054-2018 信息系统密码应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。 1、检测依据 （1）《商用密码应用安全性评估管理办法（试行）》 （2）《信息系统密码测评要求（试行）》 （3）《商用密码应用安全性评估测评过程指南（试行）》 （4）《商用密码应用安全性评估测评作业指导书（试行）》 （5）《商用密码应用安全性评估测评工具使用需求说明（试行）》 （6）《GM/T0054-2018 信息系统密码应用基本要求》 2、检测内容及分析 主要检测内容包括： （1） 物理和环境安全测评 包括：身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性等测评内容； （2） 网络和通信安全测评		

		机密性、网络边界访问控制信息的完整性、安全接入认证等测评内容； （3） 设备和计算安全测评 包括：身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性等测评内容； （4） 应用和数据安全测评 包括：身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性等测评内容； （5） 密钥管理测评 包括：密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等测评内容； （6） 安全管理测评：	整性、安全接入认证等测评内容； （3） 设备和计算安全测评 包括：身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性等测评内容； （4） 应用和数据安全测评 包括：身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性等测评内容； （5） 密钥管理测评 包括：密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等测评内容； （6） 安全管理测评： 1）管理制度测评 包括：具备密码应用安全管理制度、密钥管理规则、建立操作规程、定期修订安全管理制度、明确管理制度发布流程、制度执行	包括：身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证等测评内容； （3） 设备和计算安全测评 包括：身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性等测评内容； （4） 应用和数据安全测评 包括：身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性等测评内容； （5） 密钥管理测评 包括：密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等测评内容； （6） 安全管理测评： 1）管理制度测评		

		1）管理制度测评 包括：具备密码应用安全管理制度、密钥管理规则、建立操作规程、定期修订安全管理制度、明确管理制度发布流程、制度执行过程记录留存等测评内容； 2）人员管理测评 包括：了解并遵守密码相关法律法规和密码管理制度、建立密码应用岗位责任制度、建立上岗人员培训制度、定期进行安全岗位人员考核、建立关键岗位人员保密制度和调离制度等测评内容； 3）建设运行测评 包括：制定密码应用方案、制定密钥安全管理策略、制定实施方案、投入运行前进行密码应用安全性评估、定期开展密码应用安全性评估及攻防对抗演习等测评内容； 4）应急处置测评 包括：应急预案、事件处置、向有关主管部门上报处置情况等测评内容；结合信息系统自	过程记录留存等测评内容； 2）人员管理测评 包括：了解并遵守密码相关法律法规和密码管理制度、建立密码应用岗位责任制度、建立上岗人员培训制度、定期进行安全岗位人员考核、建立关键岗位人员保密制度和调离制度等测评内容； 3）建设运行测评 包括：制定密码应用方案、制定密钥安全管理策略、制定实施方案、投入运行前进行密码应用安全性评估、定期开展密码应用安全性评估及攻防对抗演习等测评内容； 4）应急处置测评 包括：应急预案、事件处置、向有关主管部门上报处置情况等测评内容； 结合信息系统自身的安全需求分析，通过商用密码应用安全性评估工作，发现潜在的密码应用安全隐患，形成被评估系统商用密码应用安全性评估报告，为重要网络和信息系统的密码安全提供科学评价，协助被评估单位认清	包括：具备密码应用安全管理制度、密钥管理规则、建立操作规程、定期修订安全管理制度、明确管理制度发布流程、制度执行过程记录留存等测评内容； 2）人员管理测评 包括：了解并遵守密码相关法律法规和密码管理制度、建立密码应用岗位责任制度、建立上岗人员培训制度、定期进行安全岗位人员考核、建立关键岗位人员保密制度和调离制度等测评内容； 3）建设运行测评 包括：制定密码应用方案、制定密钥安全管理策略、制定实施方案、投入运行前进行密码应用安全性评估、定期开展密码应用安全性评估及攻防对抗演习等测评内容； 4）应急处置测评 包括：应急预案、事件处置、向有关主管部门上报处置情况等测评内容； 结合信息系统自身的安全需求分析，通过商用密码应用安全性评估工作，发现潜在的密码应用		

		身的安全需求分析，通过商用密码应用安全性评估工作，发现潜在的密码应用安全隐患，形成被评估系统商用密码应用安全性评估报告，为重要网络和信息系统的密码安全提供科学评价，协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。逐步提高密码的使用能力，规避信息系统的密码安全风险。	风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。逐步提高密码的使用能力，规避信息系统的密码安全风险。	安全隐患，形成被评估系统商用密码应用安全性评估报告，为重要网络和信息系统的密码安全提供科学评价，协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。逐步提高密码的使用能力，规避信息系统的密码安全风险。		

说明：（1）投标人应按项目采购需求中的技术要求，结合自身投标情况对技术条款逐条响应。（2）当投标文件响应的技术条款完全响应招标文件要求时，投标人应注明“无偏离”；低于招标文件要求时，应注明“负偏离”；优于招标文件要求的，应注明“正偏离”。

投标人名称（公章）：广西科奥信息技术有限公司
法定代表人（负责人）或其授权代表（签字或盖章）：莫胜坤
日期：2021年 9 月 23 日

二、商务部分

（六）商务条款偏离表

商务条款偏离表

项目名称：国家税务总局广西壮族自治区税务局等级保护和风险评估服务项目
项目编号： GXJTZ[2021]110710（GX210517）　　包号：无

序号	招标文件条目号	招标文件的商务条款	投标文件的商务条款	偏离	说明
1	服务要求	（1）服务时间：本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务。 （2）服务地点：广西壮族自治区 （3）服务期限：本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务。 （4）服务方式和服务标准：提供针对本项目的技术、组织实施方案及售后服务方案。 服务方式:现场服务、电话支持 验收流程和标准，检测完成后出具相关法律法规认可的报告。 ★（5）保密要求：中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的 20%-30%的比例进行扣减。安全事件具体内容主要包括（但不限于）以下内容： （1）因补丁升级、漏洞修	**我公司承诺履行以下商务条款：** （1）服务时间：本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务。 （2）服务地点：广西壮族自治区 （3）服务期限：本项目应在签订合同之日起 1 年内完成等级保护和风险评估服务。 （4）服务方式和服务标准：提供针对本项目的技术、组织实施方案及售后服务方案。 服务方式:现场服务、电话支持 验收流程和标准，检测完成后出具相关法律法规认可的报告。 ★（5）保密要求：中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的 20%-30%的比例进行扣减。安全事件具体内容主要包括（但不限于）以下内	无偏离	/

		复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。	容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。		
2	付款方式	签订合同之日起30 日内预付合同总金额的50%；等级保护和风险评估服务完成后，甲方对项目进行验收，项目验收合格后30日内甲方向乙方支付合同剩余的50%服务费，乙方在申请付款时将同等金额、合法有效的发票开具给甲方，否则甲方有权顺延付款。	**我公司承诺履行以下商务条款：** 签订合同之日起30 日内预付合同总金额的50%；等级保护和风险评估服务完成后，甲方对项目进行验收，项目验收合格后30 日内甲方向乙方支付合同剩余的50%服务费，乙方在申请付款时将同等金额、合法有效的发票开具给甲方，否则甲方有权顺延付款。	无偏离	/
3	履约保证金	本项目不要求提供履约保证金。	**我公司承诺履行以下商务条款：** 本项目不要求提供履约保证金。	无偏离	/
4	项目分包	本项目不设置分包或转包。	**我公司承诺履行以下商务条款：** 本项目不设置分包或转包。	无偏离	/
5	验收标准	★1. 信息安全保密要求 （1）必须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度 （2）项目人员需保证遵守国家有关版权和知识产权保护的政策、法律、法规和制度。 （3）项目人员应对本项目	**我公司承诺履行以下商务条款：** ★1. 信息安全保密要求 （1）我公司严格遵守国家税务总局广西壮族自治区税务局的安全保密制度 （2）我公司项目人员保证遵守国家有关版权和知识产权保护的政策、法律、法	无偏离	/

		中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。 （4）中标供应商须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。 （5）项目人员必须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。 ★2. 中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。安全事件具体内容主要包括（但不限于）以下内容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作	规和制度。 （3）我公司项目人员对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，我公司负有连带责任。 （4）我公司与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。 （5）我公司项目人员与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。 ★2. 我公司运维人员在合同期间严格按采购人的网络安全和数据安全相关规定开展工作，由于我公司运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。安全事件具体内容主要包括（但不限于）以下内容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据		

		造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。	查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。		

说明：（1）投标人应按项目采购需求中的商务条款要求，结合自身投标情况对商务条款逐条响应。（2）当投标文件响应的商务内容完全响应招标文件要求时，投标人应注明“无偏离”；低于招标文件要求时，应注明“负偏离”；优于招标文件要求的，应注明“正偏离”。

投标人名称(公章)：广西科奥信息技术有限公司

法定代表人（负责人）或其授权代表(签字或盖章)：莫胜坤

日期：2021 年 9 月 23 日

三、投标人服务承诺（应包含售后服务承诺）

售后服务承诺

1、 技术服务

在项目实施过程中和项目实施后，我们将为用户提供相应的技术服务：

（1）技术咨询服务：项目实施过程中，针对用户提出的技术问题，提供现场咨询服务，如咨询的技术问题不能解决，也将为用户寻找相应的咨询渠道；项目实施结束后，为用户提供电话或上门的技术咨询服务。

（2）技术方案服务：为用户提供测试方案；针对用户提出的其它要求，提供其它技术方案。

2、 应急保障

在项目实施过程中，针对可能出现的情况，我们将通过应急保障机制，保证项目正常实施和用户系统的安全。

（1）风险因素的明确：检测过程中，对用户信息系统情况进行梳理，明确检测过程中的安全风险因素，做好相应的应对措施，同时告知用户。

（2）技术措施的准备：针对安全风险因素，准备相应的技术手段，一旦风险发生，及时处理。

（3）人员准备：掌握相应技术人员的联系方式，了解人员的技术能力，为应急做好准备。

（4）资源准备：了解用户和自己的相应资源。

3、 保密承诺

我们将严格对项目实施过程中涉及的用户信息进行保密。

（1）我们派出的人员已经跟单位签订有工作保密协议。

（2）根据用户项目的要求，我们可以与用户签订针对本项目的保密协议。

我们同时要求员工，在工作工程中做到：

1）未经允许，不随意进入用户的工作场所；

2）未经允许，不操作用户的设备；

3）不乱翻、乱动用户桌面的资料、文件、书籍；

4）不打听与工作无关的事情。

5）不泄露用户信息。

4、 廉洁承诺

我们承诺：

（1）不接受用户的宴请；

（2）不接受用户的礼品、烟、酒包括土特产；

（3）不接受观光旅游安排和休闲娱乐活动；

（4）不接受、索要红包。

5、 售后服务

我们非常重视售后服务工作，充分考虑用户的需求，急用户之所急，为用户提供最好的服务。

（1）服务内容

包括本次投标的所有分标的售后服务内容。包括商务条件偏离表中承诺的内容。

（2）服务响应

A、提供 7×24 小时电话技术支持（包含电话、邮件、远程桌面支持）；

B、对问题和投诉在 30 分钟内给予回应。

（3）文档

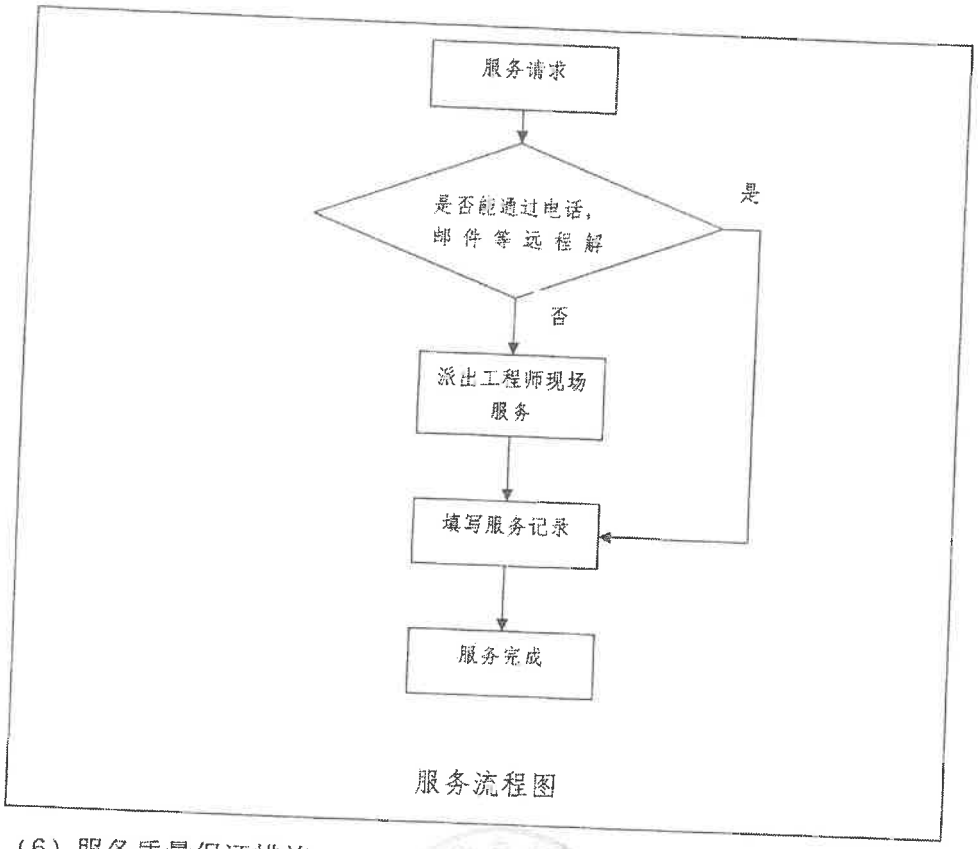
为用户提供项目检测报告有关文档。

（4）服务组织

为保证服务内容的落实和服务质量，由单位检测科负责日常服务工作，主管业务的领导负责协调。

（5）服务流程

根据服务内容的有关要求，通过清晰服务流程，提高服务质量和服务效率。同时，服务流程的清晰也为服务监督提供了依据。可以通过服务流程的控制，方便的了解服务过程，改进工作。



服务流程图

（6）服务质量保证措施

我们具有多名具有认证资质的信息安全工程师，有专业的信息技术，数据库技术，网络技术方面的技术人才；单位配备有满足信息系统测试的软件和设备；配备有交通车辆和通讯工具。能快速响应用户的请求，提供优质的服务。

单位每年都外派技术人员参加各种技术培训，内部也建立了培训制度，努力提供员工处理问题，解决问题的能力。

单位还通过加强考核管理，促进服务质量的不断提高。

（7）服务人员守则

A、文明礼貌、态度友好。

B、工作积极、及时周到。

C、未经用户同意，不乱动、操作用户设备。

D、不在用户工作场所看报纸、杂志。

E、不乱翻、乱动用户桌面的资料、文件、书籍。

F、不打听与工作无关的事情。

G、不泄露用户信息。

（8）服务监督

用户可对我方服务人员的文明礼貌、工作态度、解决和处理问题的能力等提出监督意见。我方由负责此项工作的总经理负责接受监督意见，根据用户意见，不问理由考核员工，督促用户意见的落实并回复用户。

（9）售后服务联系方式

用户所有的售后服务请求，可以通过以下方式与我们联系，我们将在最短时间内响应用户请求并提供相应服务。

(四)采购需求

第六章　项目采购需求

一、项目要求及技术需求			
序号	采购内容	数量	项目要求及技术需求
1	等级保护测评服务	1项	对国家税务总局广西自治区税务局的8个信息系统开展等级保护测评工作； 1、测评依据 （1）《安全保护等级划分准则》（GB17859-1999） （2）《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2018） （3）《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019） 2、测评内容： 须按照信息系统等级保护测评规范，制定详实的测评方案；在保证测评质量的前提下，按时完成测评工作，并提交测评报告；根据所测系统的测评报告，提供切实可行的整改技术方案，并协助用户按照技术方案做好所测系统的安全整改工作，直至清除安全隐患。 测评应包括以下内容： （1）物理安全评估：应包括机房环境和硬件设施物理安全等内容； （2）网络安全测评：应包括网络结构、网络设备及网络安全设备等内容； （3）主机安全测评：应包括操作系统及数据库系统等内容； （4）应用安全测评：应包括系统应用的身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护等内容； （5）数据安全及备份恢复测评：应包括系统数据完整性、数据保密性、备份和恢复等内容； （6）安全管理制度评估：应包括管理制度、制定和发布、评审和修订等内容； （7）安全管理机构评估：应包括岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等内容； （8）人员安全管理评估：应包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容； （9）建设管理评估：应包括系统建设的全过程，系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发等内容； （10）运维管理评估：应包括资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等内容。 3、测评方法 在安全测评过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。在招标文件中详细描述所采用的测评方法。 对信息系统进行安全漏洞检测和挖掘，检测例如缓冲区溢出、SQL注入和跨站脚本等常见安全漏洞，并提供漏洞修补建议及时采取适当的处理措施进行修补，有效阻止安全隐患被利用和发生安全事件。

2	风险评估服务	1项	对国家税务总局广西壮族自治区税务局12个重要信息系统进行风险评估，对信息系统的资产、威胁、脆弱性进行识别分析，并对现有的管理制度和技术措施进行安全评估，提高重要信息系统防范风险的能力。供应商所出具的报告需具备产品质量评价、成果及司法鉴定，具有法律效力。 1、评估目标 （1）对现有的信息安全管理制度和技术措施的有效性进行风险评估。 （2）对系统资产、威胁、脆弱性进行识别、分析。 （3）提出安全整改建议。 2、评估范围 包括：系统所涉及的物理环境、网络、主机、系统软件、应用软件、管理制度、人员等。 3、评估内容 （1）信息系统安全管理状况检查 评估各种安全制度的建立情况。包括：终端计算机访问互联网的相关制度；终端计算机接入内网的相关制度；使用移动存储介质的制度；系统业务应用人员、系统的开发、维护、管理人员、维护人员相关的安全管理制度等。 （2）网络结构、网络安全设备 评估范围包括：分析网络拓扑结构是否清晰划分网络边界；评估网络的访问控制措施。 （3）对资产的脆弱性进行收集和整理 物理环境，包括机房环境、空调、防雷接地等； 检查交换机、路由器的口令设置和管理，配置文件的备份等； 检查路由器操作系统是否存在安全漏洞；检查端口开放、管理员口令设置和管理、访问控制表；关键路由设备是否有冗余配置等。 防火墙、入侵检测系统、防病毒、桌面管理、审计等，评估安全配置的有效性。 服务器：用户口令、共享资源、系统服务安全、系统安全补丁、日志记录审计、木马检测等。 （4）应用系统 评估应用系统。 数据库：数据库系统及应用数据 操作系统：应用系统和数据库涉及到的主机操作系统。 (5) 灾难备份情况 根据信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。 4、评估依据 （1）适用的法律法规 （2）现有国际标准、国家标准、行业标准 （3）GB/T 20984-2007（信息安全技术 信息安全风险评估规范） （4）GB_T31509-2015 （信息安全技术 信息安全风险评估实施指南） （5）GB/T9361-2011 计算机场地安全要求 （6）GB17859-1999 计算机信息系统安全保护等级划分准则 （7）GB/T 18336.3-2008 信息安全技术 信息技术安全性评估准则 （8）GB/T 22081-2008 信息技术 信息安全管理实用规则

			（9）行业主管部门对业务系统的要求和制度 （10）系统相关单位的安全要求 （11）系统本身的实时性或性能要求
3	安全检查服务	1项	对国家税务总局广西壮族自治区税务局、各市税务局和各稽查局等19个单位进行安全检查，检查各单位的网络安全管理情况、安全技术防护情况、应急工作开展情况、等级保护工作落实情况、绩效相关安全工作落实情况等，指导各单位进一步健全和完善网络安全工作。 1、项目要求 通过开展信息安全检查，以查促建、以查促管、以查促改、以查促防，增强安全意识，落实安全责任，深入分析安全风险，系统评估安全状况，全面排查安全隐患，进一步健全安全管理制度，完善安全防护措施，提升自主可控水平和安全防护能力，预防和减少信息安全事件的发生，切实保障重要信息与信息系统的安全稳定运行。 2、检查依据 (1)《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号) (2)《国务院办公厅关于印发<政府信息系统安全检查办法>的通知》(国办发[2009]28号) (3)《广西壮族自治区人民政府办公厅关于做好全区政府信息系统年度安全检查工作的通知》(桂政办发[2010]145号) (4)《GM/T 0054-2018信息系统密码应用基本要求》 3、信息安全检查内容 根据工作需要重点抽查但不限于以下内容： （1）信息安全管理情况 按照国家信息安全政策和标准规范要求，建立健全信息安全管理制度及落实情况。重点检查单位信息安全主管领导、管理机构和工作人员履职情况，信息安全责任制落实及事故责任追究情况，人员、资产、采购、外包服务等日常安全管理情况，信息安全规划制定情况，信息安全从业人员情况，信息安全经费保障情况等。 （2）技术防护情况 按照国家信息安全政策和标准规范要求，建立健全技术防护体系及安全防护情况。重点检查防病毒、防攻击、防篡改、防瘫痪、防泄密措施及有效性；信息边界防护措施，互联网接入安全措施，无线信息安全防护策略；服务器、信息设备、安全设备等安全策略配置，应用系统安全功能及有效性；终端计算机、移动存储介质安全防护措施；重要数据传输、存储的安全防护措施；重要信息安全漏洞修复情况等。 (3)应急工作情况 按照国家信息与信息安全事件应急预案要求，建立健全信息安全应急工作体系情况。重点检查信息安全事件应急预案制修订情况、应急演练情况；应急技术支撑队伍、灾难备份措施建设情况；重大信息安全事件处置情况等。 (4)灾难备份情况 针对信息化项目建设时设计的灾难恢复等级，重点检查当前备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力等七大要素。

				(5)宣传教育培训情况 重点检查信息安全宣传教育、领导干部及各级人员信息安全基础培训、信息安全人员专业技术培训等情况。 (6)等级保护工作落实情况 按照国家信息安全等级保护工作标准规范和法规的要求，重点检查重要信息系统定级备案、安全测评和安全建设整改等等级保护制度落实情况。 (7)商用密码使用情况 按照国家商用密码管理标准规范和法规的要求，重点检查重要信息和信息系统中密码技术、产品和服务的使用情况。重点是信息设备中采用密码技术的情况；各类密码产品的使用情况，及其安全策略配置情况；密码应用集成商、运营商的基本情况；各重要信息与信息系统开展密码测评情况等。 (8)安全问题整改情况 上一年度各类信息安全检查所发现问题的整改情况及整改效果。
4	源代码检测服务	1项		对国家税务总局广西壮族自治区税务局8个应用系统进行应用系统源代码审计，形成源代码安全审计报告和安全功能测评报告。经评审后形成安全开发评审报告。 1、检测依据 安全检测主要依据以下标准： （1）《ISO9126 软件产品评价—质量特性及其使用指南》 （2）《GB/T 20271-2006 信息安全技术 信息系统安全通用技术要求》 （3）《GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求》 （4）《ISO9126 软件产品评价—质量特性及其使用指南》 （5）《GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求》 （6）《GBT 20988-2007 信息安全技术 信息系统灾难恢复规范》 （7）《GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范》 （8）《GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南》 （9）CVE(Common Vulnerabilities & Exposures)公共漏洞字典表 （10）OWASP 十大 Web 漏洞（Open Web Application Security Project） 本项目相关文档，包括开发实施合同、需求规格说明书、系统详细设计、部署安装详细说明说、操作手册和功能列表等 2、检测分析 （1） 静态安全性测试分析 要求采用先进的源代码审计工具对源代码进行完整的自动化审计工作，并得出结果报告，再由专业检测人员进行人工判断、分析，最终获得较为准确的软件代码安全问题结果。 源代码审计的内容包括： 1）前后台分离的运行架构 2）WEB 服务的目录权限分类 3）认证会话与应用平台的结合 4）数据库的配置规范 5）SQL 语句的编写规范 6）WEB 服务的权限配置 7）对抗爬虫引擎的处理措施 （2） 人工审查

			使用自带审查功能对源代码漏洞进行人工审查，分析排除源代码漏洞中的误报内容，同时检查真实存在漏洞代码的关联点，查看是否有漏报，分析排查后将结果生成报告并导出，作为正式报告编写的参考内容。
5	密码测评	1项	对1个信息系统进行商用密码应用安全性评估工作，根据被测信息系统当前的安全状况，给出测评结果并提出改进建议，以确保被测信息系统达到《GM/T0054-2018信息系统密码应用基本要求》的要求，也为其信息资产安全和业务持续稳定运行提供保障。 1、检测依据 （1）《商用密码应用安全性评估管理办法（试行）》 （2）《信息系统密码测评要求（试行）》 （3）《商用密码应用安全性评估测评过程指南（试行）》 （4）《商用密码应用安全性评估测评作业指导书（试行）》 （5）《商用密码应用安全性评估测评工具使用需求说明（试行）》 （6）《GM/T0054-2018信息系统密码应用基本要求》 2、检测内容及分析 主要检测内容包括： （1） 物理和环境安全测评 包括：身份鉴别、电子门禁记录数据存储完整性、视频记录数据存储完整性等测评内容； （2） 网络和通信安全测评 包括：身份鉴别、通信数据完整性、通信过程中重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证等测评内容； （3） 设备和计算安全测评 包括：身份鉴别、远程管理通道安全、系统资源访问控制信息完整性、重要信息资源安全标记完整性、日志记录完整性、重要可执行程序完整性、重要可执行程序来源真实性等测评内容； （4） 应用和数据安全测评 包括：身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性等测评内容； （5） 密钥管理测评 包括：密钥生成、密钥存储、密钥分发、密钥导入与导出、密钥使用、密钥备份与恢复、密钥归档、密钥销毁等测评内容； （6） 安全管理测评： 1）管理制度测评 包括：具备密码应用安全管理制度、密钥管理规则、建立操作规程、定期修订安全管理制度、明确管理制度发布流程、制度执行过程记录留存等测评内容； 2）人员管理测评 包括：了解并遵守密码相关法律法规和密码管理制度、建立密码应用岗位责任制度、建立上岗人员培训制度、定期进行安全岗位人员考核、建立关键岗位人员保密制度和调离制度等测评内容； 3）建设运行测评 包括：制定密码应用方案、制定密钥安全管理策略、制定实施方案、投入运行前进行密码应用安全性评估、定期开展密码应用安全性评估及攻防对抗演习等测评内容；

			4）应急处置测评 包括：应急预案、事件处置、向有关主管部门上报处置情况等测评内容； 结合信息系统自身的安全需求分析，通过商用密码应用安全性评估工作，发现潜在的密码应用安全隐患，形成被评估系统商用密码应用安全性评估报告，为重要网络和信息系统的密码安全提供科学评价，协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议，逐步提高密码的使用能力，规避信息系统的密码安全风险。
二、商务要求表			
其他要求			一、服务要求： （1）服务时间：本项目应在签订合同之日起1年内完成等级保护和风险评估服务。 （2）服务地点：广西壮族自治区 （3）服务期限：本项目应在签订合同之日起1年内完成等级保护和风险评估服务。 （4）服务方式和服务标准：提供针对本项目的技术、组织实施方案及售后服务方案。 服务方式现场服务、电话支持 验收流程和标准，检测完成后出具相关法律法规认可的报告。 ★（5）保密要求：中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。安全事件具体内容主要包括(但不限于)以下内容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。 二、付款方式：签订合同之日起30日内预付合同总金额的50%；等级保护和风险评估服务完成后，甲方对项目进行验收，项目验收合格后30日内甲方向乙方支付合同剩余的50%服务费，乙方在申请付款时将同等金额、合法有效的发票开具给甲方，否则甲方有权顺延付款。 三、履约保证金：本项目不要求提供履约保证金。 四、项目分包：本项目不设置分包或转包。 五、验收标准 ★1.信息安全保密要求 （1）必须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度 （2）项目人员需保证遵守国家有关版权和知识产权保护的政策、法律、法规和制度。 （3）项目人员应对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄

	器，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。 （4）中标供应商须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。 （5）项目人员必须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。 ★2.中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。 安全事件具体内容主要包括(但不限于)以下内容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。

（五）合同验收书格式（验收时填制，供参考）

项目验收书（付款时提供）

一、项目基本情况

（一）项目名称及编号

（二）合同名称及编号

（三）乙方名称、乙方联系人及联系方式

（四）合同金额

（五）历次验收及已付款情况等

二、项目基本内容

（一）合同约定的主要内容

（二）本次付款对应的合同内容和所属阶段

三、组织验收情况

（一）验收情况，包括验收内容、验收期限等

（二）验收评价及结论，包括项目执行情况、是否通过验收等

四、其他需要说明的情况

五、应支付合同款情况

依据验收结论，本次验收后应支付合同第几次付款及付款金额等

项目负责人签字：

验收牵头部门领导签字：

验收部门（章）

年　　月　　日

(六)政府采购项目履约保证金退付意见书（供参考）

<table>
<tr><td rowspan="3">供应商申请</td><td>项目编号：</td></tr>
<tr><td>项目名称：</td></tr>
<tr><td>该项目已于_____年_____月_____日验收并交付使用。根据合同规定，该项目的履约保证金，期限于_____年_____月_____日已满，请将履约保证金人民币（大写）_____（¥_____）退付到达以下帐户。
单位名称：
开户银行：
帐　　号：
联系人及电话：

供应商签章：
年　　月　　日</td></tr>
<tr><td>采购人意见</td><td>退付意见：（是否同意退付履约保证金及退付金额）

联系人及电话：　　采购人签章
年　　月　　日</td></tr>
</table>