

兴安盟工程建设项目审批管理系统 数据标准3.0升级项目

政府采购合同



采购包名称：兴安盟工程建设项目审批管理系统
数据标准3.0升级项目(二包)

甲 方：兴安盟住房和城乡建设局

乙 方：内蒙古思沃科技有限公司

政府采购合同

合同编号：152203-NXZC-1-CS-20260007-1-HT-2659840

甲方：兴安盟住房和城乡建设局

地址：兴安盟党政办公大楼9楼

乙方：内蒙古思沃科技有限公司

地址：呼和浩特市经济技术开发区如意总部基地水岸小镇
G-2区G1栋楼8楼



甲乙双方根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关法律法规、规范性文件，以及兴安盟工程建设项目审批管理系统数据标准 3.0 升级项目（二次）（项目名称）152203-NXZC-1-CS-20260007-1（项目编号）的中标（成交）结果、招标（磋商）文件、投标（响应）文件等文件的相关内容，经平等自愿协商一致，就如下合同条款达成一致意见。

一、项目依据

项目合法性依据，主要包括如下文件：

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字[2007]43号）；

《关于推动信息安全等级保护测评体系建设和等级测评工作的通知》（公信安[2010]303号）；

《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）。

测评技术规范依据，主要包括如下技术标准：

《信息安全技术 网络安全等级保护基本要求》
(GB/T22239-2019)；

《信息安全技术 网络安全等级保护测评过程指南》
(GB/T28449-2018)；

《信息安全技术 网络安全等级保护测评要求》
(GB/T28448-2019)。

二、服务内容

见附件一《技术要求》

乙方应以科学、客观、公正为准则，如实反映甲方信息系统的真实情况，并给出相应的测评报告，其过程和结果均不受任何第三方的干扰。

乙方依据《信息安全技术 网络安全等级保护基本要求》
(GB/T22239-2019)，分别从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心及安全管理制度等层面上对甲方被测评信息系统进行安全测评。

三、测评对象

测评系统名称：兴安工程建设审批管理系统；

所有权归属：兴安盟住房和城乡建设局；

甲方联系人：刘常海

联系电话：18447071251

乙方联系人（项目负责人）：赵瑞强

联系电话：18904711920

四、测评方式

现场测评实施期间，安全测评的主要方式为：访谈、核查和测试。



1. 访谈

访谈是指测评人员通过与信息系统有关人员(个人/群体)进行交流、讨论等活动,获取相关证据表明信息系统安全保护措施是否落实的一种方法。在访谈的范围上,应基本覆盖所有的安全相关人员类型,在数量上可以抽样。

2. 核查

核查是指测评人员通过对测评对象进行观察、查验、分析等活动,获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在检查范围上,应基本覆盖所有的对象种类(设备、文档、机制等),数量上可以抽样。

3. 测试

测试是指测评人员通过对测评对象按照预定的方法/工具使其产生特定的响应等活动,查看、分析响应输出结果,获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在测试范围上,应基本覆盖不同类型的机制,在数量上可以抽样。

五、测评开始时间、地点和期限及计划

测评时间: 自合同签订之日起, 6 个月内完成全部测评工作并提交正式测评报告;

测评地点: 兴安盟住房和城乡建设局;

交付测评报告的期限: 自合同签订之日起, 6 个月内完成全部测评工作并提交正式测评报告。

六、测评费用及其支付方式

1. 本项目测评费用(含税)共计 134,000.00 元(大写:人民币壹拾叁万肆仟元整)。支付方式如下:

(1) 合同生效且乙方提交等额合规的增值税专用发票及经



甲方书面确认的项目实施计划书后，甲方于 30 个自然日内支付合同总金额的 70%，即 93800.00 元。

(2) 项目通过最终验收（以甲方出具的书面验收合格文件为准），且乙方提交全部最终成果物及等额发票后，甲方于 30 个自然日内支付合同总金额的 30%，即 40200.00 元”。

(3) 项目结束后，乙方提供《网络安全等级测评报告》《商用密码应用安全评估报告》《软件测试报告》以上资料的纸质版。

2. 甲方以银行转帐（银行转账或支票）的方式支付上述款项，乙方提供如下信息：

收款人全称：内蒙古思沃科技有限公司

开户银行：招商银行股份有限公司呼和浩特新华广场支行

账号：471900489810801

统一社会信用代码：91150105318457836Q

七、测评费用的支付和实际测评结论无关。

如存在乙方根本违约（如测评报告严重失实、侵犯第三方知识产权等）的违约责任，包括但不限于退还全部已付款项、支付违约金并赔偿甲方全部损失。

八、双方的权利义务及违约责任

1. 甲方应按协议规定向乙方支付测评费用。
2. 甲方负责提供符合交付要求的受测信息系统及相关文档。
3. 甲方负责提供必要的协助工作，积极配合乙方测评工作。
4. 在测评项目进行过程中甲方需向乙方项目人员免费



提供测评办公环境。

5. 甲方应按本合同约定的服务项目要求,向乙方提供真实、可靠、完整的技术资料、数据和有关证件,并对其提供资料、数据的完整性、正确性、真实性、有效性负责。自本协议生效后,甲方保证5个工作日内按照系统安全测评的要求提供全部有关资料。

6. 为使乙方顺利开展工作,甲方应指定现场接待人员和技术人员,协助乙方进行现场勘察,并为乙方提供现场有关书面资料。

7. 乙方在安全测评开始之前,应通知甲方做好相应的系统数据备份等工作,并明确告知甲方测评中将要采用的方法、工具、操作步骤,将要参与的人员以及可能出现的风险,经甲方书面同意后方可进行测评操作。

8. 乙方在甲方现场测评时,应遵守甲方的工作纪律,不破坏甲方的工作设备和软、硬件设施;如果乙方对甲方的工作设备或者软、硬件设施造成破坏,应承担相应的赔偿责任。

9. 乙方应按时完成测评工作,测评完成后出具书面测评报告。乙方出具的测评报告应包括对甲方被测信息系统的检查结果及改进建议。

10 未经甲方的书面同意,乙方不得将测评事项委托给第三方。

11. 乙方完成本协议约定的所有测评工作后,由乙方方向甲方提交等级测评报告正本一份。甲方对报告的内容在收到(以电子邮件方式发出的,系统显示发送成功即视为有效送达)电子报告后的五个工作日内未提出书面意见,视为验收合格。



九、违约责任

1. 甲方逾期付款的，每逾期一工作日，应按照合同总价款的 0.1% 向乙方支付违约金，甲方逾期超过 30 工作日的，乙方有权解除合同。

2. 非因乙方原因，甲方在合同履行期间终止履行合同的，应支付此前乙方已履行部分的实际费用并应按照合同总价款的 30% 向乙方支付违约金。

3. 甲方违反本合同有关期限约定，逾期向乙方提供相关资料，本合同约定的服务期限相应顺延。

4. 甲方逾期二个月不提供或者不补充有关技术资料、数据和不配合测评工作，导致乙方无法开展工作的，乙方有权解除合同。

5. 因乙方原因逾期向甲方提交测试报告的，每逾期一工作日，应当向甲方支付合同总价款 0.1% 的违约金，乙方逾期超过 15 工作日的，甲方有权解除合同。

6. 乙方根本违约(如测评报告严重失实、侵犯第三方知识产权等)的违约责任，包括但不限于退还全部已付款项、支付违约金并赔偿甲方全部损失。

十、免责条款

1. 甲方应积极配合乙方进行测评工作，保证提供的相关资料真实可靠。非因乙方原因导致测评工作无法正常进行或按时完成，乙方不承担违约责任。

2. 甲方应在乙方开始测评前做好系统数据备份等准备工作，非因乙方的原因导致甲方经济损失的，乙方不承担责任。



3. 乙方出具的测评结论只针对甲方被测评系统在测评时的状况,不适用于该系统结构或功能等要素发生变化后的情况。

十一、保密条款

1. 双方对在本协议签订、履行过程中获知的对方的保密信息负有保密义务,并另行签署保密协议,以规范双方的保密义务。

2. 本协议及其内容亦属于保密信息的组成部分。

3. 本条款不因本协议的终止、解除而失效。

4. 一方或其工作人员违反前款规定给对方造成损失的,应当承担赔偿责任。

十二、不可抗力

1. 如果一方或双方因出现水灾、火灾、台风、地震、战争、疫情或其它不可抗力事由不能正常履行协议,须在不可抗力事由发生之日起 15 个工作日内通知对方,提供有关该事由的权威证明和书面说明。

2. 不可抗力事由发生后,双方应尽力采取措施防止损失的扩大。

3. 根据不可抗力事由对协议继续履行的影响程度,由双方协商决定是否解除协议,部分免除一方或双方义务或延期履行协议。

十三、争议解决

合同发生纠纷时,双方应协商解决,协商不成,向兴安盟人民法院起诉解决。

十四、其他

1. 本协议的未尽事宜,经双方友好协商后,可签订补充



协议，与本协议具有同等法律效力。

2. 本协议经甲乙双方签字盖章后生效。

3. 本协议一式 贰 份，甲方持有 壹 份，乙方持有 壹 份，具有同等法律效力。

4. 本协议的附件与正文具有同等法律效力。

5. 本协议的任何修改和补充都应采用书面形式，并经双方授权代表签字盖章后生效。

十六、 甲乙双方确认以下地址为往来函件的送达地址

甲方：兴安盟住房和城乡建设局

联系人：刘常海

电话：18447071251

地址：兴安盟党政综合楼

乙方：内蒙古思沃科技有限公司

联系人：王羽

电话：0471-4599573

地址：呼和浩特市经济技术开发区如意总部基地水岸小镇
G-2 区 G1 栋楼 8 楼

（以下无正文，为签字盖章页）



甲方（签章）：兴安盟住房和城乡建设局



授权代表人（签字）：



日期：2026年8月10日

乙方（签章）：内蒙古思沃科技有限公司



授权代表人（签字）：

日期：2026年8月10日



附件一 《技术要求》

序号	服务名称	技术要求																																												
1	等级保护测评	1.1 系统等级指标 三级系统：被测系统的定级结果为 S3A3 级，相对应的业务信息安全等级为 S3，系统服务安全等级为 A3；则该系统的测评指标应包括 GB/T 22239-2019 技术要求中的相应的通用指标和扩展指标。 二级系统：被测系统的定级结果为 S2A2 级，相对应的业务信息安全等级为 S2，系统服务安全等级为 A2；则该系统的测评指标应包括 GB/T 22239-2019 技术要求中的相应的通用指标和扩展指标。 1.2 测评指标 具体三级系统、二级系统测评指标内容如下表： <table><tr><th colspan="4">安全通用要求</th></tr><tr><th>类别</th><th>层面</th><th>二级</th><th>三级</th></tr><tr><td rowspan="5">技术要求</td><td>安全物理环境</td><td>15</td><td>22</td></tr><tr><td>安全通信网络</td><td>4</td><td>8</td></tr><tr><td>安全区域边界</td><td>11</td><td>20</td></tr><tr><td>安全计算环境</td><td>23</td><td>34</td></tr><tr><td>安全管理中心</td><td>4</td><td>12</td></tr><tr><td rowspan="5">管理要求</td><td>安全管理制度</td><td>6</td><td>7</td></tr><tr><td>安全管理机构</td><td>9</td><td>14</td></tr><tr><td>安全管理人员</td><td>7</td><td>12</td></tr><tr><td>安全建设管理</td><td>25</td><td>34</td></tr><tr><td>安全运维管理</td><td>31</td><td>58</td></tr><tr><td>合计</td><td>/</td><td>135</td><td>211</td></tr></table> 1.3 测评内容 从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等层面，所要求的基本安全控制在信	安全通用要求				类别	层面	二级	三级	技术要求	安全物理环境	15	22	安全通信网络	4	8	安全区域边界	11	20	安全计算环境	23	34	安全管理中心	4	12	管理要求	安全管理制度	6	7	安全管理机构	9	14	安全管理人员	7	12	安全建设管理	25	34	安全运维管理	31	58	合计	/	135	211
安全通用要求																																														
类别	层面	二级	三级																																											
技术要求	安全物理环境	15	22																																											
	安全通信网络	4	8																																											
	安全区域边界	11	20																																											
	安全计算环境	23	34																																											
	安全管理中心	4	12																																											
管理要求	安全管理制度	6	7																																											
	安全管理机构	9	14																																											
	安全管理人员	7	12																																											
	安全建设管理	25	34																																											
	安全运维管理	31	58																																											
合计	/	135	211																																											

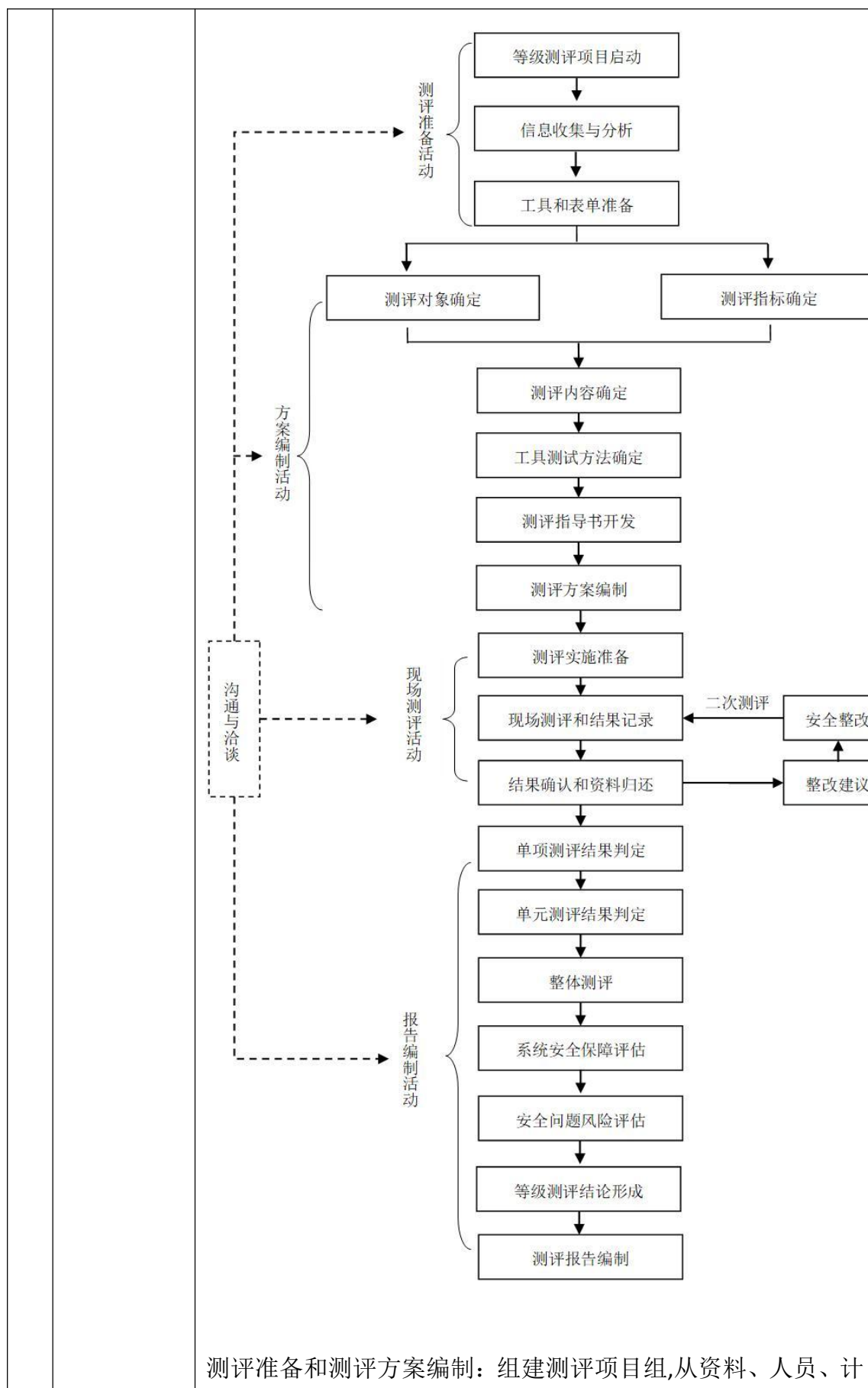


	息系统中的实施配置情况；整体测评应主要测评分析信息系统的整体安全性，内容上应包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评。 （1）安全物理环境：是针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等。 （2）安全通信网络：是针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网；涉及的安全控制点包括网络架构、通信传输和可信验证等。 （3）安全区域边界：是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证等。 （4）安全计算环境：是针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护等。 （5）安全管理中心：是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。 （6）安全管理制度：是针对整个管理制度体系提出的安全控制要求；涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订等。 （7）安全管理机构：是针对整个管理组织架构提出的安全控制要求；涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查等。 （8）安全管理人员：是针对人员管理模式提出的安全控制要求；涉
--	---



	及的安全控制点包括人员录用 、人员离岗、安全意识教育和培训以及外部人员访问管理等。 （9）安全建设管理：是针对安全建设过程提出的安全控制要求；涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用 、 自行软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理等。 （10）安全运维管理：是针对安全运维过程提出的安全控制要求；涉及的安全控制点包括环境管理、 资产管理、介质管理、设备维护管理、漏洞和风险管理、 网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理等。 1.4 测评的流程 根据国家等级保护相关标准， 安全等级保护测评流程分为四个阶段：测评准备阶段 、方案编制阶段、现场测评阶段、分析与报告编制阶段。 安全等级保护测评流程如下图所示：
--	---





		划安排等方面为等级保护测评实施做好准备,熟悉被测单位信息系统的基本信息,并编制项目计划书。根据被测信息系统的调研结果,分析被测系统及其涉及的业务应用系统,确定出本次测评的测评内容;根据已经了解到的被测系统定级结果,确定出本次测评的测评指标;测评过程中,确认现场检查的关键安全点,并且充分考虑到检查的可行性和风险,最低限度的避免对被测系统,尤其是在线运行业务系统的影响;确定现场测评的具体实施内容,即单元测评内容;最终完成测评方案的编制。 根据测评方案,按照测评标准针对测评信息系统进行测评实施,收集测评证据并分析评估,发现该系统面临的主要安全风险。 根据测评发现的网络设备、安全设备、主机系统、安全管理问题,提出安全整改或加固的建议,为招标人进行安全整改或安全加固工作提供技术指导。 整改完成后复测,根据各类测评结果记录表,分析和汇总各类测评数据,形成整体测评结论,出具被测信息系统的《网络安全等级测评报告》。
2	商用密码应用安全性评估	2.1 商用密码总体要求测评 (1) 密码算法合规性测评:信息系统中使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。 (2) 密码技术合规性测评:信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。 (3) 密码产品合规性测评:信息系统中使用的密码产品与密码模块是否通过国家密码管理部门核准。 (4) 密码服务合规性测评:信息系统中使用的密码服务是否通过国家密码管理部门许可。 2.2 密码技术应用测评 从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对信息系统中应用的密码技术进行分析与评估。



	物理和环境层面测评:分析评估信息系统是否合理、合规的利用商用密码完整性、真实性功能，对影响信息系统安全防护效能的物理和环境层面因素进行保护。包括但不限于下列典型因素：重要场所的物理访问控制，监控设备的物理访问控制，以及物理访问记录、监控信息等敏感信息数据完整性。 网络和通信层面测评:分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的网络和通信层面因素进行保护。包括但不限于下列典型因素：安全认证连接到内部网络的设备，通信双方的身份认证过程，通信数据完整性，敏感信息数据字段机密性，网络边界访问控制信息完整性，系统资源访问控制信息完整性，安全设备、安全组件的集中管理方式和信息传输通道。 设备和计算层面测评:分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的设备和计算层面因素进行保护。包括但不限于下列典型因素：登录信息系统设备和计算环境的用户身份鉴别过程，系统设备和计算环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要程序或文件完整性，信息系统设备和计算环境的日志记录完整性。 应用和数据层面测评:分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性以及不可否认性功能，对影响信息系统安全防护效能的应用和数据层面因素进行保护。包括但不限于下列典型因素：登录信息系统应用和数据操作环境的用户身份鉴别过程，系统应用和数据操作环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要数据传输过程的机密性、完整性，重要信息存储过程的机密性、完整性，重要程序的加载和卸载过程，信息系统应用相关实体行为不可否认性，信息系统应用和数据操作环境的日志记录完整性。 2.3 密钥管理测评
--	--





对影响商用密码防护效能的密钥生命周期相关环节，以及相关环节管理和策略制定的全过程进行分析与评估。密钥生命周期相关环节包括但不限于下列典型环节：密钥生成，密钥存储，密钥分发，密钥导入，密钥导出，密钥使用，密钥备份，密钥恢复,密钥归档，密钥销毁。

2.4 管理测评

对影响商用密码防护效能的管理制度与措施进行分析与评估。管理制度与措施包括但不限于下列典型维度：管理制度、人员管理、建设运行、应急处置。

（1）管理制度维度，包括但不限于密码建设、运维、人员、设备、密钥管理内容，密码相关操作规范、安全操作规范，安全管理制度的合理性和适用性论证与审定，安全管理制度的改进和修订，安全管理制度的发布，安全管理制度的执行。

（2）人员管理维度，包括但不限于了解并遵守密码相关法律法规密码产品使用，关键岗位划分，相关人员职责与权限划分,岗位责任制与人员制约、监督机制，管理和使用账号，人员培训、人员选拔，人员考核、奖惩与调离，人员保密措施。

（3）建设运行维度，包括但不限于下列内容与措施：包括但不限于信息系统规划，信息系统建设方案，信息系统密码产品、服务选用，信息系统运行前与定期评估，信息系统整改。

（4）应急处置维度，包括但不限于应急预案，应急资源准备，应急情况与处置，上级主管部门应急报告，同级密码主管部门应急报告。

2.5 测评指标

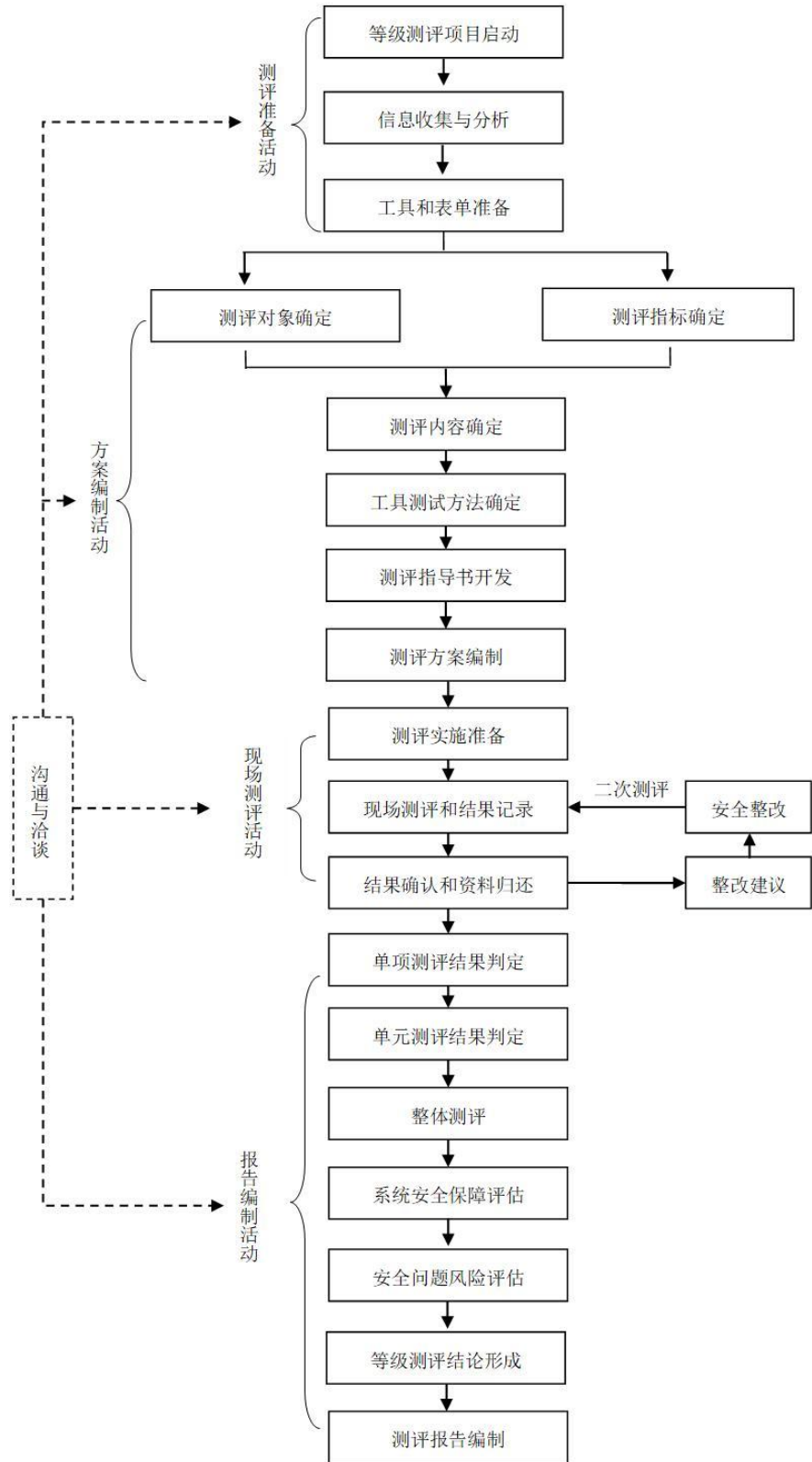
测评指标汇总表			
要求维度	安全层面	二级	三级
密码应用技术	物理和环境安全	4	5
	网络和通信安全	6	7

		要求	设备和计算安全	5	7
			应用和数据安全	8	10
		密码应用管理要求	管理制度	3	6
			人员管理	4	5
			建设运行	4	5
			应急处置	1	3
		合计	/	35	48
		2.6 测评实施原则			
		测评实施遵循以下原则：			
		1.准确性原则：测评实施时， 结合 GB/T43206 中的测评指标及相关内容开展工作，确保测评实施内容、取证结果和指标考查内容的一致性。			
		2.完备性原则：测评实施时， 考虑在不同检查点上获取证据并相互验证， 以确保取证结果是完备的。			
		3.可靠性原则：测评实施时， 结合不同类型的测评方式获取证据并相互验证， 以确保取证结果是可靠的。			
		差异性原则：针对不同的密码实现方式， 应在测评实施关注点上有所差异。若密码技术由合规密码产品实现， 检查重点在于密码产品是否被安全、正确地使用 。若密码技术由非合规产品实现， 检查重点在于密码实现（如开源密码库）是否是当前未发现明显安全问题的版本， 以及密码技术实现和使用正确性、密钥管理措施安全性等方面。			
		2.7 测评流程			
		依据《信息系统密码测评要求》、和《商用密码应用安全性评估测评过程指南》，			
		参考信息系统网络安全等级保护定级情况和 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》相关密码应用要求， 信息系统密码测评流程分为密评准备、方案编制、现场密评、分析与现场报告编制四个阶段：			



	1.测评准备活动是开展测评工作的前提和基础,主要任务是掌握被测信息系统的详细情况,准备测评工具,为编制密评方案做好准备。 2.方案编制活动是开展测评工作的关键活动,主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等,形成密评方案,为实施现场测评提供依据。 3.现场测评活动是开展测评工作的核心活动,主要任务是根据密评方案分步实施所有测评项目,以了解被测信息系统真实的密码应用现状,获取足够的证据,发现其存在的密码应用安全性问题。 分析与报告编制活动是给出测评工作结果的活动,主要任务是根据密评方案和 GM/T0 115 的有关要求,通过单元测评、整体测评、,量化评估和风险分析等方法,找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距,并分析这些差距可能导致的被测信息系统所面临的风险,从而给出各个测评对象的测评结果和被测信息系统的评估结论,形成密评报告。 测评实施流程如下:
--	--





2.8 交付物

依据 GB/T39786-2021《信息系统密码应用基本要求》等国家和行业

		商用密码相关规范标准，在服务期内，对项目中信息系统开展密码应用安全性评估，评估内容为：商用密码总体要求测评、密码技术应用测评、密钥管理测评、安全管理测评。测评后，出具加盖检测机构印章的《商用密码应用安全评估报告》。
3	软件测试	3.1 测试特性及要求 （1）功能性测试 功能测试（Functional testing）也称为行为测试（behavioral testing），根据产品特性、操作描述和用户方案，测试一个产品的特性和可操作行为以确定它们满足设计需求。功能测试是为了确保程序以期望的方式运行而按功能要求对软件进行的测试，对软件产品的所有特性和功能都进行测试确保符合需求和规范。 （2）性能效率测试 验证软件是否满足招标文件、软件开发合同、系统设计文档、软件需求规格说明或用户文档集等规定的性能要求。被测软件是否满足用户的性能需求，被测软件是否能够达到预期的系统响应时间以及业务处理时间，满足业务需求。时间特性测试应进行：响应时间、并发用户数等测试。 （3）信息安全性测试 从保密性、完整性、抗抵赖性、可核查性、真实性五个方面验证被测系统是否满足规定的安全性的要求。 （4）易用性测试 对被测软件的易安装性、用户界面的友好性、易学习性、易操作性、联机帮助丰富性等进行测试，保证系统的快速、灵活、简单的使用。 （5）兼容性测试 针对被测软件在指定的硬件配置及软件系统环境下能否正常稳定运行，而不会出现意外的退出进行测试。 （6）可靠性测试 结合功能测试寻找软件缺陷，提高被测软件的可靠性，主要针对被测软件的错误屏蔽、数据校验能力和其他与功能相关的可靠性指



	标的测试。 (7) 可移植性测试 测试被测软件对特定硬件、特定操作系统、特定数据库系统、特定支撑软件或其特定版本的依赖程度， 软件可移植、跨平台使用的能力。 (8) 维护性测试 针对被测软件在诊断缺陷、判断失效原因、标识需要修改的部分时，维护者或用户的工作量应大小， 耗费的资源多少的测试。 (9) 回归测试 BUG 修复后对于被测软件的重新验证。软件测试完毕之后， 提交问题报告单， 软件开发方对测试过程中的问题进行修复， 修复之后需对被测软件进行重新测试。 1) 验证问题是否已修复。 2) 测试修复过程中是否产生新的 BUG。 3.2 测试方法 软件测试方法包含： (1) 黑盒测试：基于系统需求规格， 在不知道系统或组件的内部结构的情况下进行的测试。通常又将黑盒测试叫做：基于规格的测试、输入输出测试、功能测试或数据驱动测试。是基于用户观点出发的测试。主要是验证功能是否符合需求， 包括原定功能的检验、是否有冗余功能、遗漏功能。 (2) 灰盒测试：静态的白盒测试或动态的黑盒测试， 灰盒就是介于黑白之间, 对软件内部有所了解, 但不见得到了如指掌的程度, 却可以结合这些了解做些比黑盒多点的测试。 (3) 白盒测试：结构测试、逻辑驱动测试或给予程序的测试。主要是分析程序的内部构造， 并根据内部构造设计测试用例。 3.3 测试工作流程 软件测试工作流程包括：测试需确认、制定测试计划、设计测试用例、执行测试用例、异常情况报告编写、 回归测试、通过判断、 出
--	--



	具报告， 测试流程如下图所示： 3.4 通过判定标准 参测系统的 “功能性、性能效率、可靠性、易用性、兼容性、可移植性、维护性、信息安全性 ” 8 大质量特性结果为 “通过 ” 的系统， 在测试报告中确定为 “通过 ” ； 对任意一项不通过的系统， 在测试报告中确定为 “不通过 ”。 评价标准如下： 1) 测试用例覆盖测试需求率达 100%； 2) 测试用例回归执行率达 100%； 3) 测试后系统没有出现致命性问题、严重性问题、一般性问题和较小性问题， 其他不影响系统正常使用的建议性问题可以存在； 4) 测试评审环节完善， 包含对测试计划、测试用例、测试记录、 回归测试记录及测试报告的测试评审。 3.5 缺陷管理 （1）评审缺陷 需对测试人员发现的缺陷进行评审。评审后如果对缺陷有疑问， 可以与测试人员沟通。对未能达成一致的缺陷由项目经理组织项目组成员评审。 （2）提交缺陷 测试人员将缺陷提交到委托方。 （3）修改缺陷 开发人员对已确认的缺陷进行修改， 填写修改记录， 修改缺陷状态为 “ 已修改 ” 或其他状态。 （4）关闭缺陷 测试人员对已修改的缺陷进行验证。如果已修改完成， 测试人员将缺陷状态设置为已修改。 3.5 测试变更 当测试需求变更， 功能变化， 测试人员根据变更情况， 评估测试变更所需时间， 提出变更风险。如变更情况被项目组通过， 测试
--	---



	人员将按上述流程进行变更测试。 3.6 测试总结 测试项目负责人应组织测试人员根据合同或其他等效文件， 被测软件文档、测试需求规格说明、测试计划、测试说明、测试记录、 问题及变更报告和软件问题报告等， 对测试工作和被测软件进行分析和评价， 并将对以后有价值的数据和文档收集整理入库，执行测试总结。 测试总结的输出是《软件测试报告》， 以及提交测试数据记录以和问题报告单。 3.7 测试报告 在被测项目整个系统测试完成之后， 依据整个测试过程形成的测试记录， 总结测试过程和测试结果， 最后出具权威的《软件测试报告》。
--	--

