项目编号 ：ZFCGHY-20240130

新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目

公 开 招 标

华域咨询
HUA YU ZI XUN
（甲级）

采购人：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）

采购代理： 新疆华域建设工程项目管理咨询有限公司

联 系 人： 李娟娟

电　　话： 13179816599

联系地址： 乌鲁木齐市五星北路194号新地园大厦13楼

目　录

招标公告.....1

第一章　投标须知.....5

第二章　合同条款.....24

第三章　采购需求.....35

第四章　投标文件格式.....91

招标公告

新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）委托，对新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目进行招标，招标方式为公开招标，欢迎合格投标人前来参加此次采购项目。

一、项目名称：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目

二、项目编号：ZFCGHY-20240130

三、采购内容：

项目名称	采购内容	技术规格、参数及要求	最高投标限价（万元）	是否允许进口产品
新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目	对信息系统实施等级保护测评，明确该系统的安全建设现状，找出存在的安全风险，分析与安全通用要求和安全扩展要求之间的差距，提出安全整改建议，并以此为基础，进一步制定安全建设整改方案，完善保护措施，使该系统满足我国关于等级保护相应级别的具体要求，增加网络和信息系统安全管理的规范性和有效性，提高单位的安全意识，增强网络抗攻击的能力，保证网络和信息系统正常运转。	详见第三章	20.00	否

四、招标方式：公开招标

五、审查方式：资格后审

六、最高投标限价：200000.00 元

七、服务期限：合同签订后 30 个工作日内（30 个工作日中不含安全整改所占时间及公安受理备案所占时间）完成以上服务并通过最终验收合格。

八、投标人资格要求：

1. 满足《中华人民共和国政府采购法》第二十二条规定；

2. 落实政府采购政策需满足的资格要求：

本项目属于专门面向中小企业采购项目，大型企业不允许参加此项目投标。

3. 本项目的特定资格要

3.1 供应商须具备公安部门颁发的《《网络安全等级测评与检测评估机构服务认证证书》；

3.2 本项目不接受联合体

九、获取时间、地点及方式：

时间：2024 年 11 月 20 日至 2024 年 11 月 27 日（上午 10:00-14:00，下午 15:00-19:00，北京时间）节假日除外；

地点：政采云平台 http://www.zcygov.cn/，在线申请获取采购文件（登录政府采购云平台 → 项目采购 → 获取招标文件→申请，审核通过后可下载招标文件，如有操作性问题，可与政采云在线客服进行咨询，咨询电话：95763）。

领取方式：供应商登录政采云平台 https://www.zcygov.cn/在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）

十、其他补充事项

1.本项目采用远程不见面电子标的方式开标。开标当日供应商无需到达开标现场，仅需通过政采云平台“不见面”开标大厅完成远程解密、询标澄清、在线多轮报价、结果公布等交互环节。

2.潜在供应商应于领取文件须提前完成注册，并在开标前成为政采云正式供应商，并完成 CA 数字证书（符合国密标准）申领。因未注册入库、未办理 CA 数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。有意向参与兵团区域电子开评标的供应商，可访问新疆数字证书认证中心官方网站（https://www.xjca.com.cn/）或下载“新疆政务通”APP 自行进行申领。如需咨询，请联系新疆 CA 服务热线 0991-2819290；

3.供应商将政采云电子交易客户端下载、安装完成后，可通过账号密码或 CA 登录客户端进行响应文件的制作。在使用政采云投标客户端时，建议使用 WIN7（64 位）及以上操作系统。客户端请至兵团政府采购网（http://ccgp-bingtuan.gov.cn/）下载专区查看，如有问题可拨打政采云客户服务热线 400-881-7190 进行咨询。如因供应商自身原因导致在规定时间内无法正常解密的（如：浏览器故障、未安装相关驱动、网络故障、加密 CA 与解密 CA 不一致

等），采购中心/代理机构不予异常处理，视为供应商自动弃标。

4.潜在供应商领取文件须提前完成注册，并在开标前成为政采云正式供应商。

十、投标文件递交截止时间：2024 年 12 月 12 日 11:00，

地址：政采云平台(https://www.zcygov.cn/)在线投标。

十一、招标人：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）

联系电话：0991-5269101

十二、采购代理机构：新疆华域建设工程项目管理咨询有限公司

联系人：王鹤宇、李娟娟

电话：0991-4630336

第一章　投标须知

投标人须知前附表

项号	条款号	编列内容	
1	1.1.1	项目名称：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目	
		项目编号：ZFCGHY-20240130	
		项目预算：20.00 万元，最高限价：20.00 万元；（投标报价超过项目预算的按无效投标处理。）	
		服务地点：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）	
		服务期限：合同签订后 30 个工作日内（30 个工作日中不含安全整改所占时间及公安受理备案所占时间）完成以上服务并通过最终验收合格。	
2	1.2.1	采购内容：对信息系统实施等级保护测评，明确该系统的安全建设现状，找出存在的安全风险，分析与安全通用要求和安全扩展要求之间的差距，提出安全整改建议，并以此为基础，进一步制定安全建设整改方案，完善保护措施，使该系统满足我国关于等级保护相应级别的具体要求，增加网络和信息系统安全管理的规范性和有效性，提高单位的安全意识，增强网络抗攻击的能力，保证网络和信息系统正常运转。**（详见第三章采购需求）**	
3	1.3.1	资金来源：自筹资金	
4	1.3.2	资金落实情况：已落实	
5	1.4.1	招标方式	公开招标
6	1.5.1	投标人的资质要求： 1. 满足《中华人民共和国政府采购法》第二十二条规定； 2. 落实政府采购政策需满足的资格要求： 本项目属于专门面向中小企业采购项目，大型企业不允许参加此项目投标。 3. 本项目的特定资格要 3.1 供应商须具备公安部门颁发的《《网络安全等级测评与检测评估机构服务认证证书》； 3.2 本项目不接受联合体	
7	1.5.2	联合体投标	本次招标不接受联合体投标。

8	3.1	投标报价方式：直接填写报价	
9	6.3	评标办法：综合评估法	
10	4.1	递交方式：电汇、转账、电子保函 保证金金额：5000.00 元； 开户单位名称：新疆华域建设工程项目管理咨询有限公司 账号：107083025521 开户银行：中国银行乌鲁木齐市南湖东路支行 开户行行号：104881006151 1.投标保证金的缴纳形式：投标保证金于投标截止时间（北京时间，以到账时间为准）之前，从投标人基本账户以银行电汇、网银的形式汇至或递交至招标 代理机构账户，各投标单位缴纳投标保证金时在附加信息及用途栏内注明“项 目名称简写”。 开完标以后，各供应商需将保证金回执单发送到 1986968236qq.com 注：1.如果发现投标单位有围标、串标行为，其响应无效，且磋商保证金将被没收，不予退还； 2.投标保证金未按规定时间缴纳或提交金额不足的,将被视为无效响应,其响应文件将不予接受。供应商应充分考虑资金在途时间）； 3.供应商递交保证金时请在汇款时注明“项目名称简称、汇款事由（投标保证金）”，对因未注明项目简称及汇款事由而造成保证金不能及时到账的，后果由供应商自负。	
11	5.2.1	投标文件的编制	1.本项目采用不见面开标，投标人需要递交电子投标文件。加密的电子投标文件 ，无需递交纸质文件。 2.开标当日，投标人无需到达开标现场，仅需通过政采云系统完成远程解密、提疑澄清、开标唱标、结果公布等交互环节。投标人必须使用能正确解密响应文件的“CA 锁”在规定的时间内完成远程解密，因投标人原因未能解密、解密失败或解密超时，视为投标人撤销其响应文件，系统内响应文件将被退回；因采购人原因或政采云平台发生故障，导致无法按时完成响应

			文件解密或开、评标工作无法进行的，可根据实际情况相应延迟解密时间或调整开、评标时间。 3.中标单位在领取中标通知书时须向采购代理机构递交纸质投标文件二份（正本一份，副本一份）、电子版投标文件一份（U 盘或者光盘），用做资料备案。 4.上述条款应按照采购文件规定的格式填写、签署和盖章。
12	5.5.1	投标文件递交	截止时间：2024 年 12 月 12 日 11 时 00 分（北京时间） 地点：线上递交，登录政采云平台 https://www.zcygov.cn/，将加密电子响应文件上传到对应项目的的指定位置
13	7.1	开标时间及地点	截止时间：2024 年 12 月 12 日 11 时 00 分（北京时间） 地点：投标人在政采云平台 https://www.zcygov.cn/不见面开标大厅远程参加开标活动
14	9.1	投标有效期	投标截止时间后 45 天
16		答疑递交截止时间	投标截止之日前十五日，投标人以电子件的形式上传至政采云平台（http://www.zcygov.cn/）
18	评标委员会的组成		评标委员会构成：5 人 评委确定方式： 政采云线上随机抽取
19	付款方式		付款方式：按医院合同执行。
20	履约担保		履约保证金金额：/ 履约保证金递交：/ 履约保证金形式：/
21	中标服务费		**本项目的招标代理服务费不足 5000 元（按 5000 元来计取）及专家评审费由中标单位支付。**
25	备注		如本投标人前附表相关内容与招标文件中的相关内容有不一致处，则以本投标人须知前附表相关内容为准。
26	项目所属行业：**软件和信息技术服务业**		

	是否专门面向中小企业采购：是 是否为本项目面向中小企业采购预留份额：是
27	需要补充的其他内容： 1.开标注意事项： （1）开标时推荐使用Chrome浏览器，且使用的电脑已经安装最新的CA驱动； （2）开标时请使用您本次加密使用的CA进行解密；开标/磋商解密时需使用CA的密码，并确开标人员已知晓正确的密码。 （3）推荐使用制作生成电子标书的电脑进行解密。 （4）开标解密路径：登录政采云平台，进入【项目采购】应用—【开标评标】菜单—【进入开标大厅】页面，找到当天开标的项目，解密时长为：30分钟。 （5）系统操作问题请咨询技术支持电话 400-881-7190，CA 办理问题请咨询新疆 CA 服务电话 0991-2819290。 2.在评标过程直至签订合同前的任何时间，如经证实发现供应商提供虚假投标资料(包括技术支持资料)或信息骗取中标的，或者未按本招标文件要求提交履约保证金的（如有要求），将取消其中标资格，没收其投标保证金，并报主管部门备案。

1、总则

1.1、概况

1.1.1、本招标项目的概况已在投标人须知前附表第 1 项中说明。

1.2、招标范围

1.2.1、本招标范围已在投标人须知前附表第 2 项中说明，投标人除非接到招标人发布的《招标文件补充》，否则不得擅自增加或删减招标范围。

1.3、资金

1.3.1、本项目的资金来源已在投标人须知前附表第 3 项说明。

1.3.2、本项目资金到位情况已在投标人须知前附表第 4 项说明。

1.4、招标方式

1.4.1、本项目招标方式已在投标人须知前附表第 5 项说明。

1.5、合格投标人

1.5.1、参加投标的投标人资质要求已在投标人须知前附表第 6 项说明。

1.5.2、招标人有权要求各投标人提供更为完整、更详细的投标人资料，以便招标人做好评审工作。

1.6、投标费用

1.6.1、投标人应承担其编制投标文件与递交投标文件所涉及的一切费用，不论投标结果如何，招标人对上述费用不做任何补偿。

2、招标文件

2.1、招标文件的组成

2.1.1、招标文件由本文件及按本文件有关规定发出的《招标文件补充》组成。

2.1.2、投标人应认真研究本招标文件所有内容，尤其应注意有**“拒绝评审”**字样的条款，否则引起的后果由投标人自负。

2.2、招标文件的解释

2.2.1、投标人在收到招标文件后，若有疑问需要澄清的，应于投标截止时间 15 天前向招标人提问，招标人将以《招标文件补充》形式予以解答。

2.3、招标文件的修改

2.3.1、投标截止日期 15 日前，招标人都可能会以招标文件补充形式修改招标文件。

2.3.2、《招标文件补充》作为招标文件的组成部分，对投标人起同等约束作用。

2.3.3、为使投标人在编制投标文件时把《招标文件补充》内容考虑进去，招标人可以延长递交投标文件的截止时间，具体时间将在《招标文件补充》中写明。

2.3.4、招标文件的澄清、修改、招标答疑会纪要等书面材料在本招标项目中均称《招标文件补充》。如果《招标文件补充》内容与在此《招标文件补充》发出之前的招标文件等书面材料中相关内容相冲突，请投标人执行《招标文件补充》的相关规定，先前发出的招标文件等书面材料中相关内容自动废止。

3、投标报价

3.1、招标项目的投标报价已在投标人须知前附表第 8 项说明。

3.2、投标人投标报价不得超过招标文件规定的本项目采购预算，未按此规定填报的投标人，整个投标文件将被视为不响应招标文件，而予以拒绝评审。

4、投标保证金

4.1、投标人在投标截止时间前，应按照投标人须知前附表第 10 项规定缴纳投标保证金。

4.2、投标人有下列情形之一者，投标保证金将被没收：

4.2.1、投标人在投标有效期内撤回其投标文件；

4.2.2、投标人不接受按招标文件规定对其投标报价进行修正的；

4.3、未中标人在中标通知书发出后 5 个工作日内，退回投标保证金。因违反规定被没收的投标保证金不予退回。

4.4、中标人的投标保证金将在合同签订之日起 5 日内返还。

4.5、投标人未按照招标文件规定缴纳投标保证金的，投标文件将被**拒绝评审**。

5、投标文件

投标人递交的投标文件应包含下列文件：正确填写的投标文件及投标文件附件、本招标文件要求投标人提供的有关资料。本文件第四章的附件所列的文件，但可以按同样格式加以扩展。

5.1、投标文件主要包括下列内容：

一、投标函
二、资格证明文件索引表
三、商务评审索引表
四、技术评审索引表
五、资格证明文件
1.法定代表人身份证明书

2.法定代表人授权委托书

3.开标一览表（附报价明细表）

4.投标人概况及资质证书

5.具备履行合同所必需的设备和专业技术能力声明函

6.商业信誉和健全的财务制度以及依法缴纳税收和社会保障资金的良好记录

7.参加采购活动前3年内，在经营活动中没有重大违法记录

8、“信用中国”、“中国政府采购网”网站查询企业信用信息截图

9、供应商必须符合法律、行政法规规定的其他条件

10、投标保证金缴纳凭证

11、资格性审查要求的其他资质证明文件

六、商务文件

1、商务条款偏离表

2、企业资质

3、类似业绩

4、人员资质及证书

5、其他商务条款证明材料

七、技术文件

1、技术条款偏离表

2、技术文件

3、测试能力

4、售后服务

5、服务流程

6、额外承诺

八、投标人认为需要提供的其他说明和资料

附件 1：中小企业声明函

5.2、投标文件的编制与签署

5.2.1、投标人必须按投标人须知前附表第 11 项规定，采用不见面开标方式。

5.2.2、开标当日，投标人无需到达开标现场，仅需通过政采云系统完成远程解密、提疑澄清、开标唱标、结果公布等交互环节。投标人必须使用能正确解密响应文件的“CA 锁”在规定的时间内完成远程解密，因投标人原因未能解密、解密失败或解密超时，视为投标人撤销其响应文件，系统内响应文件将被退回；因采购人原因或政采云平台发生故障，导致无法按时完成响应文件解密或开、评标工作无法进行的，可根据实际情况相应延迟解密时间或调整开、评标时间。。

5.2.3、**文件中凡是要求盖投标人公章和法定代表人或授权代理人签字或盖章的，必须签字或盖章上传。**

5.2.4、投标人应按照本项目采购文件和政采云平台的要求编制电子投标文件，于投标截止时间之前将制作好的加密的电子投标文件上传到“政采云”平台。未在投标文件递交截止时间前完成上传的电子响应文件视为逾期送达，逾期上传或未按规定方式上传的电子响应文件，采购单位不予受理。本项目采用不见面开标，无需提供电子响应文件U盘、纸质响应文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，联系方式：95763。

5.2.5、本项目实行网上投标，采用电子投标文件。若供应商参与投标，自行承担投标一切费用。

5.3、本项目为电子招投标，投标人需要使用CA加密设备，凡参加本项目须下载附件并填齐相关企业信息，然后发送至政采云公司指定邮箱，进行申领CA加密设备。

5.3.1、供应商将政采云电子交易客户端下载、安装完成后，可通过账号密码或CA登录客户端进行投标文件制作。客户端请至新疆政府采购网（http://www.ccgp-xinjiang.gov.cn/home.html）下载专区查看，如有问题可拨打政采云客户服务热95763进行咨询。

5.3.2、开标时间后30分钟内供应商可以登录“政采云”平台，用“项目采购-开标评标”功能进行解密响应文件。若供应商在规定时间内未按时解密的，视为响应文件撤回。

5.3.3、开标时报价签字确认时段不得超过30分钟。

5.4、迟交的投标文件视为响应文件撤回

5.4.1、各投标人应在开标前应确保成为新疆政府采购网正式注册入库供应商，并完成CA数字证书申领。因未注册入库、未办理CA数字证书等原因造成无法投标或投标失败等后果由供应商自行承担。建议于响应文件递交截止时间前1个工作日完成响应文件的制作与上传。

6、评标及定标方法

6.1评标委员会

6.1.1招标机构将按照按国家计委等七部委颁发的《评标委员会和评标方法暂行规定》及有关规定组建评标委员会。

6.1.2评标委员会由招标人和专家库中熟悉相关技术的专家组成，成员人数为五

人以上的单数，其中熟悉相关技术方面的专家不得少于成员总数的三之二。评标委员会设负责人的，评标委员会负责人由评标委员会推举产生或者由招标人确定。评标委员会负责人与评标委员会的其他成员有同等的表决权。

6.1.3 评标委员会负责评标工作，对投标文件进行审查和评估，并向招标方提交书面评标报告。

6.2、本招标项目评标定标奉行公开、公平、公正和诚实守信的原则，评标中各评委若发生意见分歧，以少数服从多数为原则决定。

6.3、本次招标项目采用综合评估法进行评标。综合评估法：评标委员会以评分方式对投标文件提出的价格部分、商务部分、技术部分、述标能否最大限度地满足招标文件中规定的各项要求和评价标准进行评估，满分共计 100 分。其中商务、技术部分 90 分，经济部分 10 分。

6.3.1、投标文件的初步评审

评标委员会将对投标人递交的电子投标文件按《投标文件资格性及符合性审查标准》进行审查。如果投标文件中有一项未通过审查标准，评标委员会将认定该投标人不通过初步评审，不得进入下一阶段评审，并且不允许投标人通过修改或撤销其不符合要求的差异或保留，使之成为具有响应性的投标。

如果投标文件初步评审造成投标人不足三个的，评标委员会应认定本次招标的投标人数量没有竞争力，宣布本次招标失败。业主方将重新组织招标活动。

表一资格性审查表：

《投标文件资格审查标准》

序号	资格审查内容	
1	具有独立承担民事责任的能力	在中华人民共和国境内注册的法人或其他组织或自然人，投标（响应）时提交有效的营业执照（或事业法人登记证或身份证等相关证明） 副本复印件，分支机构投标的，须提供总公司和分公司营业执照副本复印件，总公司出具给分支机构的授权书。
2	是否具备采购项目需要的资质条件	供应商须具备公安部门颁发的《《网络安全等级测评与检测评估机构服务认证证书》；
3	有依法缴纳税收和社会	提供投标截止日前 6 个月内任意 1 个月依法缴

	保障资金的良好记录	纳税收和社会保障资金的相关材料。 如依法免税或不需要缴纳社会保障资金的， 提供相应证明材料。
4	具有良好的商业信誉和健全的财务会计制度	供应商必须具有良好的商业信誉和健全的财务会计制度（提供 2023 年度财务状况报告或基本开户行出具的资信证明） 。
5	履行合同所必需的设备和专业技术能力	按投标（响应）文件格式填报声明函
6	参加采购活动前 3 年内，在经营活动中没有重大违法记录	参照投标（报价）函相关承诺格式内容。 重大违法记录，是指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。（根据财库〔2022〕3 号文，“较大数额罚款”认定为 200 万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于 200 万元的，从其规定）。
7	信用记录	供应商未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以资格审查人员于投标（响应）截止时间当天在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网（http://www.ccgp.gov.cn/）查询结果为准，如相关失信记录已失效，供应商需提供相关证明资料）。
8	中小企业声明函	请按照招标文件的格式正确填写《中小企业声明函》
备注：如果投标文件中有一项未通过上述审查标准，评标委员会将认定整个投标文件		

不响应招标文件而予以无效标处理，并且不允许投标人通过修改或撤销其不符合要求的差异或保留，使之成为具有响应性的投标。

表二符合性审查表：

《投标文件符合性审查标准》

序号	符合性审查内容	
1	法定代表人或授权有效签署	其《法定代表人授权书》应附在投标文件中并有效签章。
2	投标的有效期	从提交投标（响应）文件的截止之日起45日历天。
3	投标函	投标函已提交并符合招标文件格式要求的。
4	关于报价	投标报价必须是固定的，且不得以低于成本的报价投标。
5	服务期限	服务期限是否满足招标文件的要求
6	无效情形	投标文件中未有法律、法规和招标文件规定的其他无效情形。
备注：如果投标文件中有一项未通过上述审查标准，评标委员会将认定整个投标文件不响应招标文件而予以无效标处理，并且不允许投标人通过修改或撤销其不符合要求的差异或保留，使之成为具有响应性的投标。		

投标文件响应程度初步审查通过的投标企业，进入下一步详细评审阶段，未通过投标文件响应程度初步审查的投标单位，其投标作为无效标，不进入后期评审阶段。

6.3.2、投标文件的详细评审

6.3.2.1、经初步评审合格的投标文件，评标委员会应当根据招标文件确定的评标标准和方法，对其技术部分和商务部分作进一步的评审和比较。

6.3.2.2 评标委员会将对通过初步评审的投标文件进行审核，审查是否有算术或累加上的算术错误，修正错误的原则如下：

（1）若单价计算的结果与总价不一致，以单价为准修改总价；

（2）若用文字表示的数值与用数字表示的数值不一致，以文字表示的数值为准。

（3）评标委员会将按上述修正错误的方法调整投标文件中的投标报价，调整后的价格应对投标人具有约束力，如果投标人不接受对其错误的更正，其投标将被拒绝。

6.3.2.3、在评审过程中，为了有助于对投标文件进行审查、评估和比较，招标方有权向投标人质疑，请投标人澄清投标内容。投标人有责任按照招标方通知的时间、地点指派专人进行答疑和澄清。评标委员会可能要求投标人就投标文件中的内容进行答辩，招标方将以政采云线上形式通知投标人，投标人应按通知要求进行答辩。

6.3.2.4、采用 综合评估法 衡量投标文件是否最大限度地满足招标文件中规定的各项综合评分标准。评标委员会将按照《投标文件详细评分表》对通过初评的投标文件进行详细评审，其中商务、技术部分共 90 分，报价部分 10 分。

《投标文件详细评分表》

评审项目		评审内容
报价部分（10 分）		投标报价得分＝（评标基准价/投标报价）×价格分值 【注：满足招标文件要求且投标价格最低的投标报价为评标基准价。】最低报价不是中标的唯一依据。因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。
商务部分（56 分）	企业资质（13 分）	1、投标人具有在有效期内的 ISO9001 质量管理体系认证证书、ISO20000 服务管理体系认证证书、ISO27001 信息安全管理体系认证证书，提供证书复印件，每提供一个证得 1 分，全部提供得 3 分。 2、投标人同时具有 CCRC 信息系统安全运维服务资质证书和 CCRC 信息安全风险评估服务资质证书，提供证书复印件，每提供一个证得 1 分，全部提供得 2 分； 3.投标人具有智能化系统集成服务企业能力等级资质证书（一级）、信息系统售后服务企业能力等级资质证书（一级）、系统集成维保服务企业能力等级资质证书（甲级）、网络安全系统保障企业能力等级资质证书（甲级）的，每提供一个证得 2 分，全部提供得 8 分。 注：以上全部资质必须提供证书扫描件或认定结果公示截图，不提供不得分；

	类似业绩(10 分)	投标供应商提供近三年（开标截止时间前三年）类似项目业绩，一项业绩得 2 分；最高得 10 分。 注：以上业绩证明材料须提供中标通知书、合同协议书（合同扫描件至少提供封面、服务内容和签字盖章页）；
	项目人员配备（26 分）	1、拟派项目经理须由高级测评师担任，软件测评工程师（高级）、密码安全工程师（高级）、注册信息安全专业人员（CISP）证书，每满足一项得 2 分，全部满足得 6 分。（项目经理须满足高级测评师的前提，否则该项不得分。） 2、其他成员： （1）团队人员具备注册信息安全专业人员（CISP）证书的，每提供一个证书得 2 分，满分得 4 分。 （2）团队人员具有注册渗透测试工程师（CISP-PTE）证书的，每提供一个证书得 2 分，满分得 4 分。 （3）团队人员具备信息安全保障人员认证证书（CISAW）风险评估（专业级）和（CISAW）安全运维（专业级），只要具备其中一个证书得 2 分，满分得 4 分。 （4）团队人员具备软件测评工程师（高级）证书的，每提供一个证书得 2 分，满分得 4 分。 （5）团队人员具备 CCSS-M（中级）证书的，每提供一个证书得 2 分，满分得 4 分。 **注：1.投标人为上述证书人员缴纳近三个月（任意一个月即可）社保证明材料。** **2.同一人具有上述多个证书的可累计得分；** **3.需提供以上人员测评师证书复印件、资质证书复印件；**
技术部分（34 分）	服务方案(14 分)	由评委对各投标人测评技术方案进行综合评分，评分细则如下： 1、投标人按照测评需求的要求编制测评实施技术方案，内容详尽，且目标针对性、可行性强，具有完整的风险说明及风险规避处置措施，项目实施计划合理，得 7 分； 投标人编制的测评实施技术方案内容较完整，目标明确，实施计划较合理，具有较完整的风险说明及风险规避处置措施的，得 4 分； 投标人提供的测评实施技术方案内容较简单，得 2 分； 投标人提供的测评实施技术方案内容仅为概念，无具体可实施性操作的，得 0 分。 2、安全培训服务方案的理念最先进、措施最可行、安排进度最合理的，得 7 分； 安全培训服务方案的理念较先进、措施较可行、安排进度较合理的，得 4 分； 安全培训服务方案的理念先进性、措施可行性、安排进度基本合理性的，得 2 分； 无安全培训服务方案，得 0 分。

	测评设备（6 分）	投标人具备满足等级测评工作所需要的测评设备和工具。 （1）测评设备配置齐全、自备测评工具性能良好，与等保测评项目的具体特点和实际需要相契合的，得 6 分。 （2）测评设备配置较多、自备测评工具性能较好，与等保测评项目的具体特点和实际需要较符合的，得 4 分。 （3）测评设备配置不足、自备测评工具性能较差，与等保测评项目的具体特点和实际需要结合不够的，得 2 分。 （4）无相关内容，得 0 分。
	售后服务（8）	测评机构阐述内容须包含但不限于以下内容： （1）拟投入本项目售后服务人员的名单。提供人员配置名单且证明材料完整的得 2 分，否则不得分； （2）提供售后服务人员的固定电话+手机（7×24 小时）联系方式+4 小时内现场应急支撑服务承诺。提供得 2 分，未提供不得分； （3）应急响应依据甲方要求提供应急响应服务，支持网络与信息安全事件监测、发现、预警和处置，8 小时内做出实质响应。同时具有工业信息安全应急服务支撑（须提供工业信息安全应急服务支撑资质证明）的，得 2 分； （4）紧急问题处理措施，提供得 1 分，未提供不得分； （5）售后服务响应方案，提供得 1 分，未提供不得分；
	沟通反馈措施、应急、投诉处理方案（4 分）	措施科学合理、应急处理、投诉处理方案针对性较强得 4 分，措施较合理、应急处理、投诉处理方案针对性一般得 2 分，措施不合理、应急处理、投诉处理方案针对性一般得 1 分，未作应答得 0 分。
	服务流程（6 分）	阐述内容须包含但不限于以下内容： （1）阐述测评服务整体流程； （2）针对测评过程中重点难点的应答； 横向对比所有测评机构的应答，阐述内容涵盖全部，标准清晰、针对性较强、方案、措施完善、可行性较高得 6 分；阐述内容基本涵盖全部，标准清晰、针对性较强强、方案、措施完善、可行性一般得 4 分；阐述内容未涵盖全部，标准清晰、对不同专业工程的阐针对性一般、方案、措施完善、可行性一般得 2 分；未提供不得分。
	额外承诺（3 分）	考察测评机构是否提供额外承诺；投标供应商承诺组织专业人员提供一年至少两次的安全培训服务，培训内容包括：1.等保 2.0 技术要求、2.涉密网络建设标准及技术要求、3、风险评估过程要求等；每提供一项得 1 分，满分 3 分，未提供不得分。
备注：1.评委应在认真理解本招标文件和项目有关情况后，做出需自己负责的按上述内容对投标人进行评审。 2.投标人得分为所有评委打分算术平均值。		

6.3.3.5、投标人最终得分等于商务、技术部分与经济部分得分之和，如果出现

投标人最终得分相同的情况，投标报价低者排名顺序优先在前。

6.3.3.6、评标委员会按照投标人最终得分由高到底顺序确定出各投标人排名顺序。

6.4、定标原则

6.4.1、评标委员会对投标文件初步评审的投标人，商务、技术部分与经济部分得分之和由高到低排序，得分最高为第一中标候选人，以此类推，确定出前三名作为中标候选人推荐给招标人，招标人从三名中标候选人中确定出最终的中标人。

6.4.2、招标人确定中标人时的原则：排名第一的中标候选人为中标人。排名第一的中标候选人放弃中标、因不可抗力提出不能履行合同，确定排名第二的中标候选人为中标人。排名第二的中标候选人因前款规定的同样原因不能签订合同的，确定排名第三的中标候选人为中标人。

7、开标时间、地点

7.1、招标项目开标的时间、地点已在投标人须知前附表第 13 项说明。

7.2、本项目采用不见面开标方式。

8、开标会程序

8.1 采购人在规定的投标截止时间（开标时间）和投标须知前附表规定的地点进行不见面远程开标。供应商的法定代表人或企业负责人或其委托代理人无需到达开标现场，仅需在任意地点登录政采云平台 https://www.zcygov.cn/进入“政采云远程开标大厅”参加开标会议，并使用 CA 密钥完成远程解密、提疑澄清、开标唱标、结果公布等交互环节。

8.2 开标时，各供应商应在规定的解密时间（30 分钟）内对本单位加密的电子投标文件进行解密，如因供应商自身原因导致在规定时间内无法正常解密的（如：浏览器故障、未安装相关驱动、网络故障、加密 CA 与解密 CA 不一致等），采购中心/代理机构不予异常处理，视为供应商自动弃标。

8.3开标时，采购代理机构将通过“政采云远程开标大厅”系统公布供应商名称、投标价格，以及采购代理机构认为合适的其它详细内容。供应商若有报价和优惠未被唱出，应在开标时及时声明或提请注意，否则采购代理机构对此不承担任何责任。

提示：开标时，请供应商随时关注政采云账号内的站内信；投标项目授权代表的手机短息（系统会推送短信至投标项目授权代表的手机），但此短信仅系友情提示，并不具有任何约束性和必要性，采购代理机构不承担供应商未收到短信而引起

的一切后果和法律责任。

8.3、评标准备会

8.3.1、采购代理机构向评标专家提供评标时的重要信息和数据。其中包括：招标的目标、范围和性质；采购文件中规定的主要技术要求、标准和商务条款；采购文件规定的评标标准、评标方法和在评标过程中考虑的相关因素。

8.4、评标委员会对投标文件依据《投标文件完备性及符合性审查标准》进行初评。

8.5、评标委员会对通过初评的投标文件依据《投标文件-评审标准》进行详细评审。

9、投标有效期

9.1、评标和定标将在投标人须知前附表第 14 项规定内完成，如果不能完成，招标人应通知投标人延长投标有效期。

10、授予合同

10.1、招标人应当按评委会推荐中标供应商排序，招标人应以排名第一的中标候选人为中标人。排名第一的中标候选人放弃中标或因不可抗力提出不能履行合同，或者招标文件规定应当提交履约保证金而在规定的期限内未能提交的，招标人可以确定排名第二的中标候选人为中标人。排名第二的中标候选人因前款规定的同样原因不能签订合同的，招标人可以确定排名第三的中标候选人为中标人。

11、合同签订

11.1、招标人与中标人在自中标通知书发出之日起 30 日内，依据《中华人民共和国经济合同法》和招标文件、投标文件签订合同。

12、质疑的提出及处理

政府采购供应商（以下简称供应商）提出质疑和投诉应当坚持依法依规、诚实信用原则。

12.1 质疑的提出

12.1.1 供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以电子件的形式上传至政采云平台 http://www.zcygov.cn/，（登录政府采购云平台）询问质疑投诉 → 质疑→提交，须按文件规定要求提交质疑。

质疑供应商应按照财政部制定的《政府采购质疑函范本》格式（可从新疆政府

采购网官方网站下载）和《政府采购质疑和投诉办法》的要求，在法定质疑期内以纸质形式提出质疑，针对同一采购程序环节的质疑应一次性提出。超出法定质疑期的、重复提出的、分次提出的或内容、形式不符合《政府采购质疑和投诉办法》的，采购人或其委托的采购代理机构将不予受理，质疑供应商将依法承担不利后果。

供应商应知其权益受到损害之日，是指：（1）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日。（2）对采购过程提出质疑的，为各采购程序环节结束之日。（3）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

12.1.2 提出质疑的供应商（以下简称质疑供应商）应当是参与所质疑项目采购活动的供应商。

潜在供应商已依法获取其可质疑的采购文件的，可以对该文件提出质疑。对采购文件提出质疑的，应当在获取采购文件或者采购文件公告期限届满之日起 7 个工作日内提出。

12.1.3、供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

提出质疑时，必须按照“实事求是”、“谁主张，谁举证”的原则，提供相关证明材料，不能主观臆测。

12.1.4 供应商可以授权委托人进行质疑和投诉。其授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

代理人提出质疑和投诉，应当提交供应商签署的授权委托书。

12.1.5 以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有供应商共同提出。

12.1.6 质疑必须提供合法的信息来源或有效证据。质疑人捏造事实、提供虚假材料或者以非法手段取得证明材料进行质疑的，将不予受理。质疑人应当保证所提出的质疑内容及相关证明材料的真实性及来源的合法性，并承担相应的法律责任。属于须由相关部门调查、鉴定或者先行做出相关认定的事项，质疑人应当依法申请具有法定职权的部门查清、认定，并将相关结果提供给招标方。招标方不具有法定调查、认定权限和义务。

12.1.7 证明材料要具备客观性、关联性、合法性，无法查实的（如宣传册、媒体报道、猜测、推理等）不能作为证明材料。

12.1.8 对不能提供相关证明材料的、涉及商业秘密的、非书面形式送达的、匿名的质疑将不予受理。

12.2 受理和处理

12.2.1 《质疑函》必须由质疑方的法定代表人（负责人）或参与本次投标的被授权人以电子扫描件的形式上传至政采云平台 http://www.zcygov.cn/。

12.2.2 采购人、采购代理机构不得拒收质疑供应商在法定质疑期内发出的质疑函，应当在收到质疑后 7 个工作日内作出答复，并以电子扫描件形式通知质疑供应商和其他有关供应商。

12.2.3 质疑答复的内容不得涉及商业秘密。

12.2.4 对于不符合上述 12 项所述的相关条款要求的质疑，招标方将不予受理。

12.2.5 在处理过程中，发现需要质疑人进一步补充相关佐证材料的，要求质疑人在规定时间内提供。质疑人不能按照要求提供相关佐证材料的，视同放弃质疑。

12.2.6 招标方或采购单位负责对质疑的回复工作，将质疑人的质疑材料提供给相关专家或评审小组，并将处理意见回复质疑人。

12.2.7 采购人、采购代理机构认为供应商质疑不成立，或者成立但未对中标、成交结果构成影响的，继续开展采购活动；认为供应商质疑成立且影响或者可能影响中标、成交结果的，按照下列情况处理：

（1）对采购文件提出的质疑，依法通过澄清或者修改可以继续开展采购活动的，澄清或者修改采购文件后继续开展采购活动；否则应当修改采购文件后重新开展采购活动。

（2）对采购过程、中标或者成交结果提出的质疑，合格供应商符合法定数量时，可以从合格的中标或者成交候选人中另行确定中标、成交供应商的，应当依法另行确定中标、成交供应商；否则应当重新开展采购活动。

质疑答复导致中标、成交结果改变的，采购人或者采购代理机构应当将有关情况书面报告本级财政部门。

12.3 质疑无效的处理

12.3.1 质疑人提供的相关佐证材料不能证明质疑成立的，招标方可要求质疑人补充相关佐证材料，如补充材料仍不能证明质疑成立的，将不予受理。

12.3.2 对于质疑人在质疑期间不配合进行质疑调查处理的，视为自动放弃质疑。

12.3.3 质疑人提出的质疑，经评标专家审定后驳回的，列为无效质疑。

12.3.4 对于质疑中使用虚假材料或恶意方式质疑的，按无效质疑处理，并列入不良记录供应商名单。

12.3.5 质疑人进行质疑后，招标方在法定时间内对质疑进行回复，质疑人认为回复不满意的，可向相关的采购管理部门进行投诉。

12.4 其他

12.4.1 质疑函和投诉书应当使用中文。质疑函和投诉书的范本，由财政部制定。

12.4.2 对在质疑答复和投诉处理过程中知悉的国家秘密、商业秘密、个人隐私和依法不予公开的信息，财政部门、采购人、采购代理机构等相关知情人应当保密。

质疑函制作说明：

1.供应商提出质疑时，应上传质疑函和必要的证明材料。

2.质疑供应商若授权委托人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一标项进行质疑，质疑函中应列明具体标项号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

第二章　合同条款（模版）

以最终签订的合同为准

新疆维吾尔自治区第二济困医院
（新疆维吾尔自治区第五人民医院）
服务合同

合同编号：

签约地：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区第五人民医院）

甲方（买方）：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区第五人民医院）

乙方（卖方）：

1.甲乙双方根据《中华人民共和国民法典》，在平等互利、协商一致的基础上，由招标代理机构:新疆华域建设工程项目管理咨询有限公司进行招标，项目编号为:ZFCGHY-20240130 的中标通知书，甲方同意向乙方购买新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目

2.甲乙双方在本合同中约定合作的事项主要包括以下表格内信息系统的等级测评服务。

服务明细：

测评对象	安全保护等级	服务报价（元）
自治区第二济困医院医院信息管理系统（HIS）	三级	
自治区第二济困医院电子病历系统（EMR）	三级	
自治区第二济困医院影像归档和通信系统（PACS）	二级	
自治区第二济困医院实验室信息管理系统（LIS）	二级	
小写含税合计金额（人民币）：	大写含税合计金额（人民币）：	

2.服务交付期

乙方应在合同签订后 30 个工作日内（30 个工作日中不含安全整改所占时间及公安受理备案所占时间）完成以上服务并通过最终验收合格。逾期将按照**第 7.2 条**规定执行。

3.服务内容

3.1 合同签订后，甲乙双方各派代表组成项目管理小组，管理本项目的所有服务，双方在合理、维护双方利益的基础上讨论项目相关事宜。

3.2 在合同签订后 5 个工作日内，甲方配合乙方对待测系统进行初步调研及后续工作安排、编制等保测评方案。

3.3 乙方负责建立健全测评工作中所涉及到的文档。

3.4 现场测评结束后乙方在 10 个工作日内编制《网络安全等级保护差距分析及整改建议》，待甲方整改完成后，甲方联系第三方进行整改施工方进行整改，乙方在复测后根据综合测评结果出具《网络安全等级保护测评报告》。

3.5 乙方应严格按照国家等级保护制度的相关标准和要求，开展网络安全等级保护测评工作，并协助甲方完成在公安部门的等级保护定级与备案工作，提交等级测评报告。

4.质量保证及售后服务

4.1 乙方承诺测评工作要通过公安机关网络安全检查无问题。

4.2 乙方严格按照国家标准进行网络安全等级保护测评工作。

4.3 乙方严格遵守保密协议中的相关约定，做好双方信息的保密工作。

4.4 乙方在甲方指定的地点开展测评工作。

4.5 乙方指派工作经验丰富的项目经理，结合技术领先、结论可靠的测评工具为甲方做全面的安全测评。

4.6 乙方按照标准性、规范性、可控性、整体性、最小影响性及保密性的原则指导下，开展等级保护测评工作，做到守时保质。

4.7 乙方在实施关键测评项时（如漏洞扫描或工具测试等），要与甲方充分沟通该关键测评项实施的细节与步骤，得到甲方许可后，再开展该测评项，以该测评项对甲方的信息系统影响最小化为目标。

5.付款方式

5.1 签订合同后甲方支付乙方总货款的 **30%，** 乙方完成本次等级测评备案工作，编制完成符合公安机关要求的网络等级测评报告验收合格后支付总货款的 **30%**，通过公安机关网络安全检查无问题，后支付总货款的 **30%**，剩余 **10%**为履约保证金，待 202 年度新疆公安机关网络安全检查工作截止后一次性无息付清。

特别约定：若 202 年度甲方未被抽到检查，则第三笔 30%于 202 年 月支付，第四笔 10%于 202 年 12 月支付。

5.2 当本合同约定的其他付款条件成就之后或同时，乙方应当根据国家税收法律规定向甲方开具合格发票，甲方在收到乙方发票原件后向乙方支付货款，若乙方不开具合格发票，则甲方有权拒绝支付货款。

5.3 中标金额包含项目产生的一切费用，甲方不再另行支付。

6.权利与义务

6.1 乙方所提供的技术服务必须符合国家法律法规、国家（行业）标准的相关要求。

6.2 乙方保证按照合同规定的时间和方式向甲方提供服务，并协助甲方尽可能的弥补缺陷。

6.3 甲方项目负责人负责协调甲方相关技术人员，为乙方提供本合同项下所需要的资源，包括但不限于工作场地、打印机、电源、访问网络设备和主机设备的权限及其他相关资料，并对上述资料的合法性、真实性、合规性承担责任。

6.4 乙方在甲方现场开展测评活动，应遵守甲方的作息制度与办公制度。乙方人员在甲方工作期间应当严格遵守甲方的各项规章制度，服从乙方负责人和甲方的管理，如因乙方人员给甲方或者第三方造成损失的，乙方应当承担全部赔偿责任。

6.5 乙方工作人员如在甲方工作期间发生受伤的，由乙方负责解决并承担全部责任，甲方不承担任何责任。

7.违约条款

7.1如经相关监督管理机构检验确认以上项目不符合本合同约定或甲方验收时发现不符合规定的，甲方有权要求乙方进行补救：

7.2 如果乙方没有按照合同规定的时间交货和提供服务，甲方有权从合同货款中扣除误期赔偿费，延期交货和延期服务的赔偿费均按每延期一日扣除延期交付部分的合同价的百分之零点五（0.5%）计算，直至交货或提供服务为止；超过 30 日仍未能交货或提供服务的，甲方有权解除合同，乙方应向甲方支付合同总额 30%的违约金。

7.3 乙方在为甲方提供安装、调试、系统对接等服务时，应当确保不会影响甲方其他系统、设备的正常运行，如因此造成甲方其他系统、软件、设备无法运营或发生断电、断网等情形的，乙方应当全额赔偿甲方的损失，该损失包括但不限于：修理、重做、更换、重新调试的相关费用，财产和权益的直接减少，财产权益应当增加而未能增加的部分，数据丢失重新补录的时间和人力损失，为维权而产生的诉讼、仲裁、调查取证费用、差旅费、律师费等。

7.4 乙方应保证甲方和使用单位在使用该设备或其任何一部分时免受第三方提出侵犯其专利权、商标权或工业产权的起诉。

7.5 乙方依据本合同约定应当承担的各项违约金和损失赔偿，甲方均有权从应支付乙方的款项中扣除。

8.争议的解决方式

甲、乙双方发生争议时，应先协商解决。协商不能达成一致，任何一方均可依法向甲方住所地人民法院提起诉讼。

9.合同生效

9.1 本合同根据招投标文件、中标通知书及谈判会议上的答疑记录等均作为合同的附件进行审核签订，是本合同不可分割的组成部分，均与本合同具有同等的法律效力。

9.2 本合同在甲、乙双方签字盖章后生效。

9.3 本合同一式**捌**份，以中文书就，甲方执**陆**份、乙方执**贰**份，具有相同的法律效应。

10.其他

10.1 招标文件、乙方投标文件与本合同具有同等法律效力。

10.2 本合同所列地址、联系方式是双方确定的作为本合同项下合同履行、争议解决方式条款中所涉仲裁法律文书的送达地址和联系方式。本合同履行过程中送达的文书包括但不限于商业函件、开庭传票、开庭通知书、证据、判决书、裁定书、裁决书、调解书、执行裁定书等。

10.3 双方确认：上述送达地址和电子邮箱适用于合同履行完毕或争议经或仲裁、一审、二审、再审、执行阶段，至案件执行程序终结时止。

10.4 任何一方发生地址、接收人变动的，应书面向对方送达并获得对方书面确认，否则不发生送达地址、接收人变动的效力；向本合同约定地址送达导致诉讼仲裁文书未能被当事人实际接收，邮寄送达的，以文书退回之日视为送达之日；直接送达的，送达人当场在送达回证上记明情况之日视为送达之日。

甲方：新疆维吾尔自治区第二济困医院　　**乙方：**

（新疆维吾尔自治区第五人民医院）（盖章）　　**（盖章）**

甲方法定代表人：_____　　**乙方法定代表人：**_____

委托代理人：_____　　**委托代理人：**

联系人：_____　　**联系人：**

联系电话：_____　　**联系电话：**

地址：乌鲁木齐喀什西路 159 号　　**地址：**

日期：2024 年　　月　　日　　**日期：**

附件一：

保密协议

甲方（买方）：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区第五人民医院）

乙方（卖方）：

鉴于乙方为甲方提供的：新疆维吾尔自治区第二济困医院（新疆维吾尔自治区中西医结合医院、新疆维吾尔自治区第五人民医院）医院信息网络等级保护测评项目，在工作过程中，乙方能够接触货总甲方获得资料、文档、和相关业务数据等保密信息，可以访问相关软件、硬件平台环境，为确保对甲方的信息系统、设备以及软、硬件平台环境有关信息进行有效保护，经双方协商，达成本协议。

一、保密信息

1.保密信息：在乙方为甲方提供服务过程中，由于工作需要从甲方获得或接触到的业务数据、连接方式及登录信息、以及工作过程中产生的各类具有保密要求的资料文档，无论以何种形式何种载体，无论在披露时时候以口头、图像或者以书面方式，均属于保密信息范围。

2.保密人员范围：甲乙双方所有参与本项目的有关人员。

3.保密期限：不论本合同是否变更、接触、种植，长期有效。

4.保密责任：赔偿对方因泄密造成的经济损失，直至追究法律责任。

二、甲方的权利与义务

1.甲方获得或知晓的乙方秘密信息，仅用于本合同内容或双方沟通需要，甲方有义务保守乙方秘密信息，不得向任何第三方泄漏。

2.甲方对乙方提供的各种介质中的各种资料负有保密费任，包括但不限于：合同、等级测评流程、作业指导书、现场测评记录表、工具测试记录表、信息系统安全等级测评报告、整改建设方案及所有与项目相关的过程文档资料，并保证不进行未经授权的节选、复印、翻译和转发；

3. 甲方由于自身其它需要，确需节选、复印、翻译和转发乙方所提供的资料时，需向乙方提出书面申请，获得乙方书面同意后，

方可使用。

4. 乙方为本合同所提供的全部资料，甲方均只在直接相关人员中传阅，且有义务在项

目结束后交回乙方或根据乙方要求销毁。

5. 甲方承诺，其接触并知悉上述秘密信息的员工负有保密义务，甲方通过一定的书面手段保证上述承诺。

三、乙方的权利与义务

1.乙方获得或知晓的甲方秘密信息，仅用于本合同内容或双方沟通需要，乙方有义务保守甲方秘密信息，不得向任何第三方泄漏。

2.乙方对甲方提供的各种介质中的各种资料负有保密责任，包括但不限于：业务数据、连接方式及登录信息、以及所有与项目相关的过程文档资料，并保证不进行未经授权的节选、复印、翻译和转发；

3.乙方由于自身其它需要，确需节选、复印、翻译和转发甲方所提供的资料时，需向甲方提出书面申请，获得甲方书面同意后，方可使用。

4.甲方为本合同所提供的全部资料，乙方均只在直接相关人员中传阅，且有义务在项目结束后交回甲方或根据甲方要求销毁。

5. 乙方承诺，其接触并知悉上述秘密信息的员工负有保密义务，乙方通过一定的书面手段保证上述承诺。

6. 乙方保证对甲方所提供的保密信息按本协议约定予以保密，并采取适用且完善的保护措施进行保密。如果由于乙方保管不当或对员工教育不力而导致保密信息流失、泄露，造成的一切后果由乙方承担。

7.乙方人员在甲方所在地工作期间，应注意甲方所提供的办公环境的安全，避免个人办公设各被他人利用，进而破坏保密信息和系统安全

8.乙方人员如需对软、硬件平台应用系统进行操作，需向甲方提出申请，甲方同意后在甲方的监督下方可进行。

四、经双方书面确认，任何一方不得变更或修改本协议附件。

五、本协议附件一式捌份，甲方陆份，乙方贰份，随合同生效而生效，与协议具有同等的法律效力。

甲方：新疆维吾尔自治区第二济困医院　　乙方：

（新疆维吾尔自治区第五人民医院）（盖章）　　（盖章）

甲方法定代表人：_____　　乙方法定代表人：_____

联系人：_____　　联系人：

联系电话：_____　　联系电话：

日期：_____　　日期：

第三章 采购需求

项目测评方案

依据（GB 17859-1999）《计算机信息系统 安全保护等级划分准则》、（GB/T 28449-2018）《信息安全技术 网络安全等级保护测评过程指南》、（GB/T 20984-2022）《信息安全技术 信息安全风险评估方法》、（GB/T 22239-2019）《信息安全技术 网络安全等级保护基本要求》、（GB/T 28448-2019）《信息安全技术 网络安全等级保护测评要求》、（GB/T 25058-2019）《信息安全技术 网络安全等级保护实施指南》、（GB/T 22080-2016）《信息技术安全技术 信息安全管理体系要求》、（GAT 390-2002）《计算机信息系统安全等级保护通用技术要求》、（GB/T 20269-2006）《信息安全技术 信息系统安全管理要求》、（GB/T 25070-2019）《信息安全技术 网络安全等级保护安全设计技术要求》、（T/ISEAA 001-2020）《网络安全等级保护测评高风险判定指引》，对信息系统实施等级保护测评，明确该系统的安全建设现状，找出存在的安全风险，分析与安全通用要求和安全扩展要求之间的差距，提出安全整改建议，并以此为基础，进一步制定安全建设整改方案，完善保护措施，使该系统满足我国关于等级保护相应级别的具体要求，增加网络和信息系统安全管理的规范性和有效性，提高单位的安全意识，增强网络抗攻击的能力，保证网络和信息系统正常运转。

1.项目总体理解及实施方案

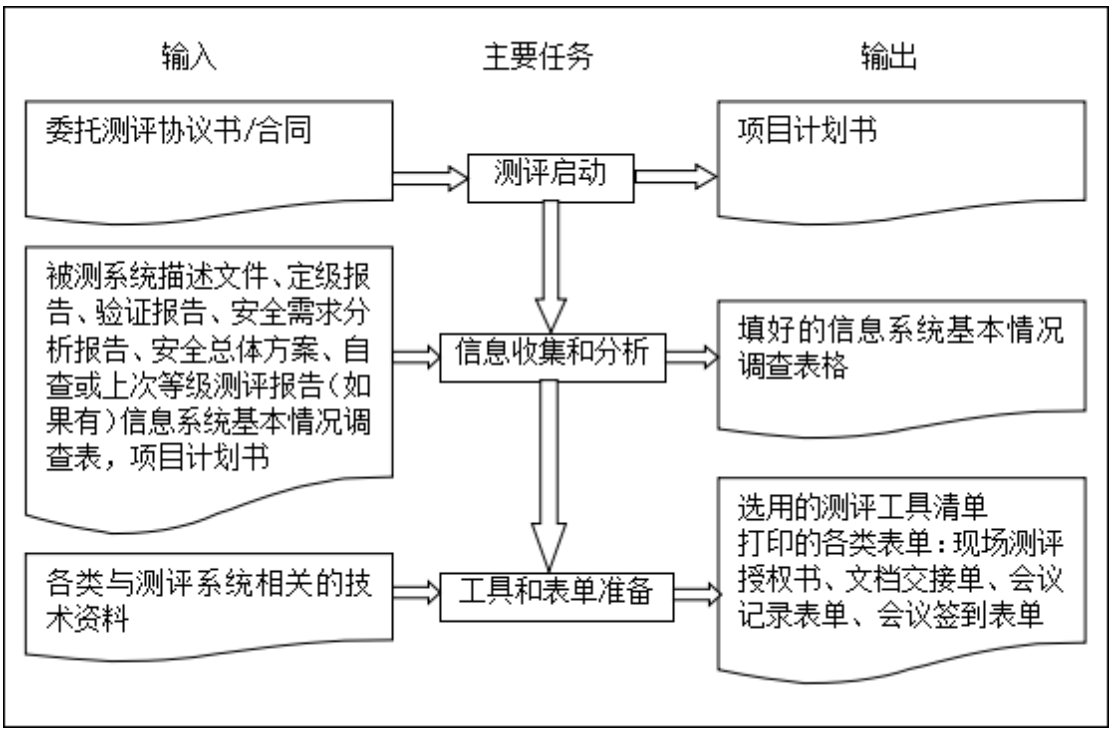
检查被测系统的安全等级保护状况是否达到相应等级的基本要求。根据对现场测评结果分析、汇总后形成《网络安全等级保护测评报告》，说明信息系统存在的安全问题。

为明确软件开发的需求，对委托单位进行详细的分析和规划，对人员分工和环境搭建进行细致的安排，利用手工和自动化的检测手段，准确的判定各部分的功能，保证系统检测的准确性。对委托单位检测工作中的时间、人员、环境、等进行拆分检测。按照委托单位需求完成对其的检测工作。

1.1 测评准备活动

测评准备阶段是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

测评准备阶段工作流程如下图所示：



测评准备阶段服务管理流程

测评准备阶段内容分为工作启动、信息收集和分析、工具和表单准备。在工作启动任务中,测评机构组建等级测评项目组,获取测评委托单位及定级对象的基本情况,从基本资料、人员、计划安排等方面为整个等级测评项目的实施做好充分准备。 测评准备阶段内容分为工作启动、信息收集和分析、工具和表单准备。

工作启动:

输入:委托测评协议书。

任务描述:

a) 根据测评双方签订的委托测评协议书和系统规模,测评机构组建测评项目组,从人员方面做好准备,并编制项目计划书。

b) 测评机构要求测评委托单位提供基本资料,为全面初步了解被测定级对象准备资料。

输出/产品:项目计划书。

信息收集和分析:

测评机构通过查阅被测定级对象已有资料或使用系统调查表格的方式,了解整个系统的构成和保护情况以及责任部门相关情况,为编写测评方案、开展现场测评和安全评估工作奠定基础。

输入:项目计划书,系统调查表格,被测定级对象相关资料。

任务描述:

a) 测评机构收集等级测评需要的相关资料,包括测评委托单位的管理架构、技术体系、运行情况、建设方案、建设过程中相关测试文档等。云计算平台、物联网、移动互联、工业控制系统的补充收集内容见附录 C 。

b) 测评机构将系统调查表格提交给测评委托单位,督促被测定级对象相关人员准确填写调查表格。

c) 测评机构收回填写完成的调查表格,并分析调查结果,了解和熟悉被测定级对象的实际情况。

这些信息可以参考自查报告或上次等级测评报告结果。

在对收集到的信息进行分析时,可采用如下方法:

1) 采用系统分析方法对整体网络结构和系统组成进行分析,包括网络结构、对外边界、定级对象的数量和级别、不同安全保护等级定级对象的分布情况和承载应用情况等;

2) 采用分解与综合分析方法对定级对象边界和系统构成组件进行分析,包括物理与逻辑边界、硬件资源、软件资源、信息资源等;

3) 采用对比与类比分析方法对定级对象的相互关联进行分析,包括应用架构方式、应用处理流程、处理信息类型、业务数据处理流程、服务对象、用户数量等。

d) 如果调查表格信息填写存在不准确、不完善或有相互矛盾的地方,测评机构应与填表人进行沟通和确认,必要时安排一次现场调查,与相关人员进行面对面的沟通和确认,确保系统信息调查的准确性和完整性。

输出/产品:填好的调查表格,各种与被测定级对象相关的技术资料。

工具和表单准备:

测评项目组成员在进行现场测评之前,应熟悉被测定级对象、调试测评工具、准备各种表单等。

输入:填好的调查表格,各种与被测定级对象相关的技术资料。

任务描述:

a) 测评人员调试本次测评过程中将用到的测评工具,包括漏洞扫描工具、渗透性测试工具、性能测试工具和协议分析工具等。

b) 测评人员在测评环境模拟被测定级对象架构,为开发相关的网络及主机设备等测评对象测评指导书做好准备,并进行必要的工具验证。

c) 准备和打印表单,主要包括:风险告知书、文档交接单、会议记录表单、会议签到表单等。

输出/产品:选用的测评工具清单,打印的各类表单。

测评准备活动中双方职责

测评机构职责:

a) 组建等级测评项目组。

b) 指出测评委托单位应提供的基本资料。

c) 准备被测定级对象基本情况调查表格,并提交给测评委托单位。

d) 向测评委托单位介绍安全测评工作流程和方法。

e) 向测评委托单位说明测评工作可能带来的风险和规避方法。

f) 了解测评委托单位的信息化建设以及被测定级对象的基本情况。

g) 初步分析系统的安全状况。

h) 准备测评工具和文档。

测评委托单位职责:

a) 向测评机构介绍本单位的信息化建设及发展情况。

b) 提供测评机构需要的相关资料。

c) 为测评人员的信息收集工作提供支持和协调。

d) 准确填写调查表格。

e) 根据被测定级对象的具体情况,如业务运行高峰期、网络布置情况等,为测评时间安排提供适宜的建议。

f) 制定应急预案。

表 1：本阶段工作任务及主要文档

任务	输入文档	任务描述	输出文档
工作启动	工作启动	工作启动	
信息收集和分析	委托测评协议书（服务合同）	1.收集等级测评需要的相关资料，包括测评委托单位的方针文件、规章制度及相关过程管理记录、被测信息系统描述文件、定级报告、安全方案、安全现状评估报告等； 2.将系统调查表格提交给测评委托单位进行填写，并对确认表单内容的准确性。	填好的调查表格、各种与被测信息系统相关的技术资料
工具和文档准备	作业指导书	1.测评人员调试本次测评过程中将用到的测评工具； 2.测评人员模拟被测评信息系统搭建测评环境； 3.准备和打印表单。如风险告知	选用的测评工具清单 打印的各类表单：风险告知书、文档

		书、会议签到表单等。	交接单、会议记录表单、会议签到表单

1.2 方案编制阶段

方案编制阶段是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

□测评对象确定

根据系统调查结果,分析整个被测定级对象业务流程、数据流程、范围、特点及各个设备及组件的主要功能,确定出本次测评的测评对象。

输入:填好的调查表格,各种与被测定级对象相关的技术资料。

任务描述:

a) 识别并描述被测定级对象的整体结构

根据调查表格获得的被测定级对象基本情况,识别出被测定级对象的整体结构并加以描述。

b) 识别并描述被测定级对象的边界

根据填好的调查表格,识别出被测定级对象边界及边界设备并加以描述。

c) 识别并描述被测定级对象的网络区域

一般定级对象都会根据业务类型及其重要程度将定级对象划分为不同的区域。根据区域划分情况描述每个区域内的主要业务应用、业务流程、区域的边界以及它们之间的连接情况等。

d) 识别并描述被测定级对象的主要设备

描述系统中的设备时以区域为线索,具体描述各个区域内部署的设备,并说明各个设备主要承载的业务、软件安装情况以及各个设备之间的主要连接情况等。

e) 确定测评对象

结合被测定级对象的安全级别和重要程度,综合分析系统中各个设备和组件的功能、特点,从被测定级对象构成组件的重要性、安全性、共享性、全面性和恰当性等几方面属性确定出技术层面的测评对象,并将与被测定级对象相关的人员及管理文档确定为测评对象。

f) 描述测评对象

描述测评对象时,根据类别加以描述,包括机房、业务应用软件、主机操作系统、数据库管理系统、网络互联设备、安全设备、访谈人员及安全管理文档等。

输出/产品:测评方案的测评对象部分。

测评指标确定

根据被测定级对象定级结果确定出本次测评的基本测评指标,根据测评委托单位及被测定级对象业务自身需求确定出本次测评的特殊测评指标。

输入:填好的调查表格,行业规范,业务需求文档。

任务描述:

a) 根据被测定级对象的定级结果,包括业务信息安全保护等级和系统服务安全保护等级,得出被测定级对象的系统服务保证类(A 类)基本安全要求、业务信息安全类(S 类)基本安全要求以及通用安全保护类(G 类)基本安全要求的组合情况。

b) 根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况,从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标。

c) 根据被测定级对象实际情况,确定不适用测评指标。

d) 根据测评委托单位及被测定级对象业务自身需求,确定特殊测评指标。

e) 对确定的基本测评指标和特殊测评指标进行描述,并分析给出指标不适用的原因。

输出/产品:测评方案的测评指标部分。

测评内容确定

本条确定现场测评的具体实施内容,即单项测评内容。

输入:填好的系统调查表格,测评方案的测评对象部分,测评方案的测评指标部分。

任务描述:

依据 GB/T22239,将前面已经得到的测评指标和测评对象结合起来,将测评指标映射到各测评对象上,然后结合测评对象的特点,说明各测评对象所采取的测评方法。由此构成可以具体实施测评的单项测评内容。测评内容是测评人员开发测评指导书的基础。

输出/产品:测评方案的测评实施部分。

测试工具接入点确定

在等级测评中,应使用测试工具进行测试,测试工具可能用到漏洞扫描器、渗透测试工具集、协议分析仪等。物联网、移动互联、工业控制系统的补充测试内容见附录 C 。

输入:测评方案的测评实施部分,GB/T22239,选用的测评工具清单。

任务描述:

a) 确定工具测试环境,根据被测系统的实时性要求,可选择生产环境或与生产环境各项安全配置 相同的备份环境、生产验证环境或测试环境作为工具测试环境。

b) 确定需要进行测试的测评对象。

c) 选择测试路径。测试工具的接入采取从外到内,从其他网络到本地网络的逐步逐点接入,即:测试工具从被测定级对象边界外接入、在被测定级对象内部与测评对象不同区域网络及同一网络区域内接入等几种方式。

d) 根据测试路径,确定测试工具的接入点。从被测定级对象边界外接入时,测试工具一般接在系统边界设备(通常为交换设备)上。在该点接入漏洞扫描器,扫描探测被测定级对象设备对外暴露的安全漏洞情况。在该接入点接入协议分析仪,捕获应用程序的网络数据包,查看其安全加密和完整性保护情况。在该接入点使用渗透测试工具集,试图利用被测定级对象设备的安全漏洞,跨过系统边界,侵入被测定级对象设备。从系统内部与测评对象不同网络区域接入时,测试工具一般接在与被测对象不在同一网络区域的内部核心交换设备上。在该点接入扫描器,直接扫描测试内部各设备对本单位其他不同网络所暴露的安全漏洞情况。在该接入点接入网络拓扑发现工具,探测定级对象的网络拓扑情况。在系统内部与测评对象同一网络区域内接入时,测试工具一般接在与被测对象在同一网络区域的交换设备上。在该点接入扫描器,在本地直接测试各被测设备对本地网络暴露的安全漏洞情况。一般来说,该点扫描探测出的漏洞数应该是最多的,它说明设备在没有网络安全保护措施下的安全状况。

e) 结合网络拓扑图,描述测试工具的接入点、测试目的、测试途径和测试对象等相关内容。

输出/产品:测评方案的工具测试方法及内容部分。

□测评指导书开发

测评指导书是具体指导测评人员如何进行测评活动的文档,应尽可能详实、充分。

输入:测评方案的单项测评实施部分、工具测试内容及方法部分。

任务描述:

a) 描述单个测评对象,包括测评对象的名称、位置信息、用途、管理人员等信息。

b) 根据 GB/T28448 的单项测评实施确定测评活动,包括测评项、测评方法、操作步骤和预期结果等四部分。测评项是指 GB/T22239 中对该测评对象在该用例中的要求,在 GB/T28448 中对应每个单项测评中的“测评指标”。测评方法是指访谈、核查和测试三种方法,具体参见附录 E。核查具体到测评对象上可细化为文档审查、实地察看和配置核查,每个测评项可能对应多个测评方法。操作步骤是指在现场测评活动中应执行的命令或步骤,涉及到测试时,应描述工具测试路径及接入点等。预期结果是指按照操作步骤在正常的情况下应得到的结果和获取的证据。

c) 单项测评一般以表格形式设计和描述测评项、测评方法、操作步骤和预期结果等内容。整体测评则一般以文字描述的方式表述,以测评用例的方式进行组织。

d) 根据测评指导书,形成测评结果记录表格。

输出/产品:测评指导书,测评结果记录表格。

□测评方案编制

测评方案是等级测评工作实施的基础,指导等级测评工作的现场实施活动。测评方案应包括但不局限于以下内容:项目概述、测评对象、测评指标、测评内容、测评方法等。

输入:委托测评协议书,填好的调研表格,各种与被测定级对象相关的技术资料,选用的测评工具清单,GB/T22239 或行业规范中相应等级的基本要求,测评方案的测评对象、测评指标、单项测评实施部分、工具测试方法及内容部分等。

任务描述:

a) 根据委托测评协议书和填好的调研表格,提取项目来源、测评委托单位整体信息化建设情况及被测定级对象与单位其他系统之间的连接情况等。

b) 根据等级保护过程中的等级测评实施要求,将测评活动所依据的标准罗列出来。

c) 参阅委托测评协议书和被测定级对象情况,估算现场测评工作量。工作量根据测评对象的数量和工具测试的接入点及测试内容等情况进行估算。

d) 根据测评项目组成员安排,编制工作安排情况。

e) 根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排。

f) 汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿。

g) 评审和提交测评方案。测评方案初稿应通过测评项目组全体成员评审,修改完成后形成提交稿。然后,测评机构将测评方案提交给测评委托单位签字认可。

h) 根据测评方案制定风险规避实施方案。

输出/产品:经过评审和确认的测评方案文本,风险规避实施方案文本。

方案编制活动中双方职责

测评机构职责:

a) 详细分析被测定级对象的整体结构、边界、网络区域、设备部署情况等。

b) 初步判断被测定级对象的安全薄弱点。

c) 分析确定测评对象、测评指标、确定测评内容和工具测试方法。

d) 编制测评方案文本,并对其进行内部评审。

e) 制定风险规避实施方案。

测评委托单位职责:

a) 为测评机构完成测评方案提供有关信息和资料。

b) 评审和确认测评方案文本。

c) 评审和确认测评机构提供的风险规避实施方案。

d) 若确定不在生产环境开展测评,则部署配置与生产环境各项安全配置相同的备份环境、生产验证环境或测试环境作为测试环境。

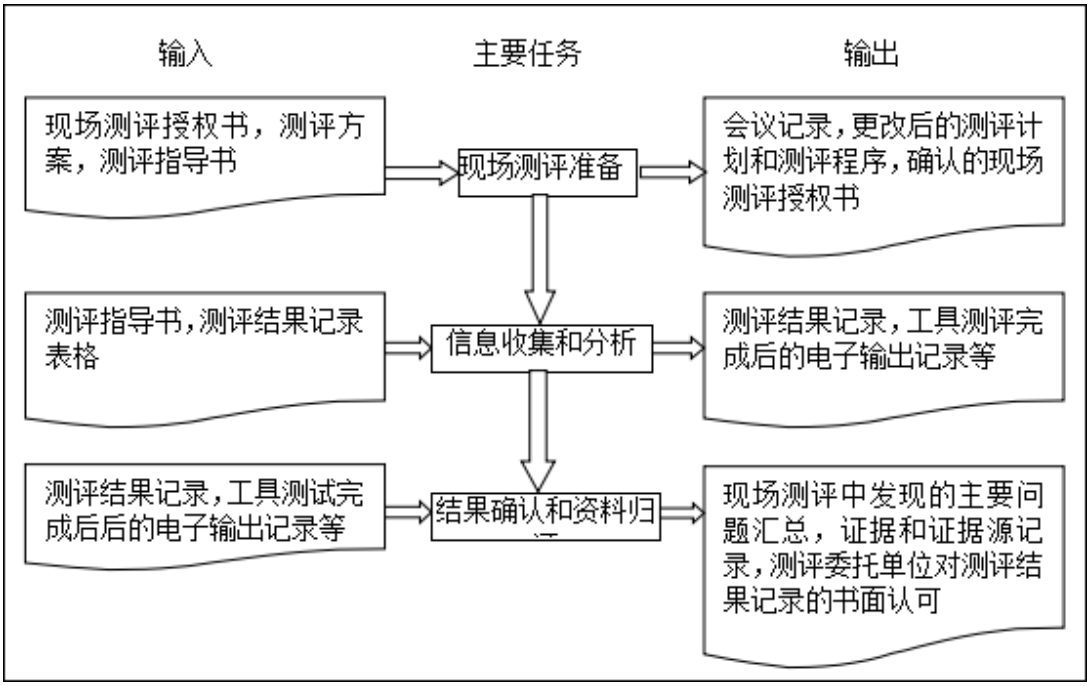
表 2：本阶段工作任务及主要文档

任务	输入文档	任务描述	输出文档
测评对象确定	填好的调查表格	1.识别并描述被测信息系统的整体结构 2.识别并描述被测信息的边界 3.确定并描述统被测信息系统的网络区域 4.识别并描述信息系统的主要设备 5.描述被测评系统 6.确定测评对象 7.描述测评对象	测评方案的测评对象部分
测评指标确定	填好的调查表格 GB/T22239-2019 或行业标准	1.根据被测评系统的定级结果，得出被测评信息系统的 SAG 的组合情况； 2.根据被测评系统的 SAG 组合情况，从 GB/T22239-2019 或行标中选择相应等级的基本安全要求作为测评指标。	测评方案的测评指标部分
测评内容确定	填好的调查表格、测评方案的测评对象和测评指标部分，GB/T 28449-2018 或行业标准	1.依据 GB/T 28448-2019 或行标，将前面已经得到的测评指标和测评对象结合起来，将测评指标映射到各测评对象上，然后结合测评对象的特点，说明各测评对象采取的测评方法，如此构成一个个可以具体实施测评的单元。	测评方案的单元测评实施部分
工具测试方法确定	测评方案的单元测评实施部分，GB/T28449-2018 或行业标准	1.选择测试路径； 2. 根据测试路径，确定测试工具的接入点； 3. 结合网络拓扑图，采用图示的方式描述测试工具的接入点、测试目的、测试途径和测试对象等相关内容。	测评方案的工具测试方法及内容部分
测评指导书	测评方案的单元	1.描述单个测评对象；	测评指

任务	输入文档	任务描述	输出文档
开发	测评实施部分、工具测试内容及方法部分	2.根据 GB/T 28448-2019 或行标的单元测评实施确定测评活动； 3. 单元测评一般以表格形式设计和描述测评项、测评方法、操作步骤和预期结果等内容； 4. 根据测评指导书，形成测评结果记录表格。	导书，测评结果记录表格
测评方案编制	委托测评协议书，填好的调研表格、各种与被测信息系统相关的技术资料	1.根据委托测评协议书和填好的调研表格，提取项目相关信息； 2.罗列依据、估算现场测评工作量； 3.编制工作安排、编制具体测评计划； 4.形成测评方案文稿，提交评审；	经过评审和确认的测评方案文本

1.3 现场测评

本项目现场测评严格按照《信息安全技术 信息系统安全等级保护测评过程指南》（GB/T 28449-2018）要求开展现场测评。现场测评阶段是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格按照测评指导书执行，分步实施所有测评项目，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。现场测评阶段工作流程如下图所示：



现场测评阶段流程图

□现场测评准备

本任务启动现场测评,是保证测评机构能够顺利实施测评的前提。

输入:经过评审和确认的测评方案文本,风险规避实施方案文本,风险告知书,现场测评工作计划。

任务描述:

a) 测评委托单位对风险告知书签字确认,了解测评过程中存在的安全风险,做好相应的应急和备份工作。

b) 测评委托单位协助测评机构获得定级对象相关方的现场测评授权。

c) 召开测评现场首次会,测评机构介绍现场测评工作安排,相关方对测评计划和测评方案中的测评内容和方法等进行沟通。

d) 测评相关方确认现场测评需要的各种资源,包括测评配合人员和需要提供的测评环境等。

输出/产品:会议记录,测评方案,现场测评工作计划和风险告知书,现场测评授权书等。

□现场测评和结果记录

本任务主要是测评人员按照测评指导书实施测评,并将测评过程中获取的证据源进行详细、准确记录。

输入:现场测评工作计划,现场测评授权书,测评指导书,测评结果记录表格。

任务描述:

a) 测评人员与测评配合人员确认测评对象中的关键数据已经进行了备份。

b) 测评人员确认具备测评工作开展的条件,测评对象工作正常,系统处于一个相对良好的状况。

c) 测评人员根据测评指导书实施现场测评,获取相关证据和信息。现场测评一般包括访谈、核查和测试三种测评方式,具体参见附录 E。

d) 测评结束后,测评人员与测评配合人员及时确认测评工作是否对测评对象造成不良影响,测评对象及系统是否工作正常。

输出/产品:各类测评结果记录。

□结果确认和资料归还

本任务主要是将测评过程中得到的证据源记录进行确认,并将测评过程中借阅的文档归还。

输入:各类测评结果记录,工具测试完成后的电子输出记录。

任务描述:

a) 测评人员在现场测评完成之后,应首先汇总现场测评的测评记录,对漏掉和需要进一步验证的内容实施补充测评。

b) 召开测评现场结束会,测评双方对测评过程中得到的证据源记录进行现场沟通和确认。

c) 测评机构归还测评过程中借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认。

输出/产品:经过测评委托单位确认的测评证据和证据源记录。

现场测评活动中双方职责

测评机构职责:

a) 测评人员开展测评前确认被测定级对象具备测评工作开展的条件,测评对象工作正常。

b) 测评人员利用访谈、文档审查、配置核查、工具测试和实地察看的方法开展现场测评工作,并获取相关证据。

测评委托单位职责：

a) 测评前备份系统和数据,并了解测评工作基本情况。

b) 协助测评机构获得现场测评授权。

c) 安排测评配合人员,配合测评工作的开展。

d) 对风险告知书进行签字确认。

e) 配合人员如实回答测评人员的问询,对某些需要验证的内容上机进行操作。

f) 配合人员协助测评人员实施工具测试并提供有效建议,降低安全测评对系统运行的影响。

g) 配合人员协助测评人员完成业务相关内容的问询、验证和测试。

h) 配合人员对测评证据和证据源进行确认。

i) 配合人员确认测试后被测设备状态完好。

测评机构职责:

a) 测评人员开展测评前确认被测定级对象具备测评工作开展的条件,测评对象工作正常。

b) 测评人员利用访谈、文档审查、配置核查、工具测试和实地察看的方法开展现场测评工作,并获取相关证据。

测评委托单位职责(系统部署在公有云的测评委托单位职责还包括附录 C 中相关内容):

a) 测评前备份系统和数据,并了解测评工作基本情况。

b) 协助测评机构获得现场测评授权。

c) 安排测评配合人员,配合测评工作的开展。

d) 对风险告知书进行签字确认。

e) 配合人员如实回答测评人员的问询,对某些需要验证的内容上机进行操作。

f) 配合人员协助测评人员实施工具测试并提供有效建议,降低安全测评对系统运行的影响。

g) 配合人员协助测评人员完成业务相关内容的问询、验证和测试。

h) 配合人员对测评证据和证据源进行确认。

i) 配合人员确认测试后被测设备状态完好。

表 3：本阶段工作任务及主要文档

任务	输入文档	任务描述	输出文档
现场测评准备	经过评审和确认的测评方案文本、风险规避实施方案文本、风险告知书、现场测评工作计划	1.测评委托单位对风险告知书进行确认； 2.召开测评首次现场会，测评机构介绍现场测评安排，双方对测评方案和测评计划中的测评内容和方法进行沟通，委托单位对测评方案认可后，签字确认； 3.测评双方确认现场测评需要的各种资源，包括测评委托单位的配合人员和需要提供的测评环境等。	会议记录,测评方案现场测评工作计划和风险告知书
现场测评和结果记录	现场测评工作计划，测评指导书，测评结果记录表格	1.测评人员和测评委托单位的配合人员确认测评对象中的关键数据已经进行了备份； 2.测评人员确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状态； 3.测评人员根据测评指导书实施现场测评； 4.测评结束后，测评人员和测评委托单位配合人员及时确认测评工作是否对测评对象造成了不良影响，测评对象及系统是否工作正常。	各类测评结果记录 测评人员根据测评指导书实施现场测评时一般包括访谈、检查和测试 3 种测评方式
结果确认和资料归还	各类测评结果记录，工具测试完成后的电子输出记录	1.测评人员在现场测评完成之后，应首先汇总现场测评的测评记录，对漏掉和需要进一步验证的内容实施补充测评；	经过测评委托单位确认的测评证据和证据源记录

		2.召开现场结束会，测评双方对测评过程中得到的证据源记录进行现场沟通和确认； 3.测评机构归还测评过程中借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认。	

1.4 分析与报告编制阶段

分析与报告编制阶段是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《等级测评过程指南》（GB/T 28449-2018）的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结果。

□单项测评结果判定

本任务主要是针对单个测评项,结合具体测评对象,客观、准确地分析测评证据,形成初步单项测评结果,单项测评结果是形成等级测评结论的基础。

输入:经过测评委托单位确认的测评证据和证据源记录,测评指导书。

任务描述:

a) 针对每个测评项,分析该测评项所对抗的威胁在被测定级对象中是否存在,如果不存在,则该测评项应标为不适用项。

b) 分析单个测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分。

c) 如果测评证据表明所有要求内容与预期测评结果一致,则判定该测评项的单项测评结果为符合;如果测评证据表明所有要求内容与预期测评结果不一致,判定该测评项的单项测评结果为不符合;否则判定该测评项的单项测评结果为部分符合。

输出/产品:测评报告的等级测评结果记录部分。

□单元测评结果判定

本任务主要是将单项测评结果进行汇总,分别统计不同测评对象的单项测评

结果,从而判定单元测评结果。

输入:测评报告的等级测评结果记录部分。

任务描述:

a) 按层面分别汇总不同测评对象对应测评指标的单项测评结果情况,括测评多少项,符合要求的多少项等内容。

b) 分析每个控制点下所有测评项的符合情况,给出单元测评结果。单元测评结果判定规则如下:

———控制点包含的所有适用测评项的单项测评结果均为符合,则对应该控制点的单元测评结果为符合;

———控制点包含的所有适用测评项的单项测评结果均为不符合,则对应该控制点的单元测评结果为不符合;

———控制点包含的所有测评项均为不适用项,则对应该控制点的单元测评结果为不适用;

———控制点包含的所有适用测评项的单项测评结果不全为符合或不符合,则对应该控制点的单元测评结果为部分符合。

输出/产品:测评报告的单元测评小结部分。

□整体测评

针对单项测评结果的不符合项及部分符合项,采取逐条判定的方法,从安全控制点间、层面间出发考虑,给出整体测评的具体结果。

输入:测评报告的等级测评结果记录部分和单项测评结果。

任务描述:

a) 针对测评对象“部分符合”及“不符合”要求的单个测评项,分析与该测评项相关的其他测评项能否和它发生关联关系,发生什么样的关联关系,这些关联关系产生的作用是否可以“弥补”该测评项的不足或“削弱”该测评项实现的保护能力,以及该测评项的测评结果是否会影响与其 有关联关系的其他测评项的测评结果。

b) 针对测评对象“部分符合”及“不符合”要求的单个测评项,分析与该测评项相关的其他层面的测评对象能否和它发生关联关系,发生什么样的关联关系,这些关联关系产生的作用是否可以“弥补”该测评项的不足或“削弱”该测评项实现的保护能力,以及该测评项的测评结果是否会影响与其有关联关系的其他测评项的测

评结果。

c) 根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值。

输出/产品:测评报告的整体测评部分。

□系统安全保障评估

综合单项测评和整体测评结果,计算修正后的安全控制点得分和层面得分,并根据得分情况对被测定级对象的安全保障情况进行总体评价。

输入:测评报告的等级测评结果记录部分和整体测评部分。

任务描述:

a) 根据整体测评结果,计算修正后的每个测评对象的单项测评结果和符合程度得分。

b) 根据各对象的单项符合程度得分,计算安全控制点得分。

c) 根据安全控制点得分,计算安全层面得分。

d) 根据安全控制点得分和安全层面得分,总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况。

输出:测评报告的系统安全保障评估部分。

□安全问题风险分析

测评人员依据等级保护的相关规范和标准,采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测定级对象安全造成的影响。

输入:填好的调查表格,测评报告的单项测评结果、整体测评部分。

任务描述:

a) 针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题,结合关联测评对象和威胁,分析可能对定级对象、单位、社会及国家造成的安全危害。

b) 结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果。

c) 根据最大安全危害严重程度进一步确定定级对象面临的风险等级,结果为“高”“中”或“低”。

输出:测评报告的安全问题风险分析部分。

□等级测评结论形成

测评人员在系统安全保障评估、安全问题风险评估的基础上,找出系统保护现状与 GB/T22239 之间的差距,并形成等级测评结论。

输入:测评报告的系统安全保障评估部分、安全问题风险评估部分。

任务描述:

根据单项测评结果和风险评估结果,计算定级对象综合得分,并得出等级测评结论。

等级测评结论分为三种情况:

a) 符合:定级对象中未发现安全问题,等级测评结果中所有测评项的单项测评结果中部分符合和 不符合项的统计结果全为 0,综合得分为 100 分。

b) 基本符合:定级对象中存在安全问题,部分符合和不符合项的统计结果不全为 0,但存在的安全问题不会导致定级对象面临高等级安全风险,且综合得分不低于阈值。

c) 不符合:定级对象中存在安全问题,部分符合项和不符合项的统计结果不全为 0,而且存在的安全问题会导致定级对象面临高等级安全风险,或者综合得分低于阈值。

输出/产品:测评报告的等级测评结论部分。

□测评报告编制

根据报告编制活动各分析过程形成等级测评报告。等级测评报告格式应符合公安机关发布的《信息安全等级保护测评报告模版》(模版示例参见附录 F) 。

输入:测评方案,《网络安全等级保护测评报告模版》,测评结果分析内容。

任务描述:

a) 测评人员整理前面几项任务的输出/产品,按照《网络安全等级保护测评报告模版》编制测评报告相应部分。每个被测定级对象应单独出具测评报告。

b) 针对被测定级对象存在的安全隐患,从系统安全角度提出相应的改进建议,编制测评报告的问题处置建议部分。

c) 测评报告编制完成后,测评机构应根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息,对测评报告进行评审。

d) 评审通过后,由项目负责人签字确认并提交给测评委托单位。

输出/产品:经过评审和确认的被测定级对象等级测评报告。

报告编制活动中双方职责

测评机构职责:

a) 分析并判定单项测评结果和整体测评结果。

b) 分析评价被测定级对象存在的风险情况。

c) 根据测评结果形成等级测评结论。

d) 编制等级测评报告,说明系统存在的安全隐患和缺陷,并给出改进建议。

e) 评审等级测评报告,并将评审过的等级测评报告按照分发范围进行分发。

f) 将生成的过程文档(包括电子文档)归档保存,并将测评过程中在测评用介质和测试工具中生成或存放的所有电子文档清除。

测评委托单位职责:

a) 签收测评报告。

b) 向分管公安机关备案测评报告。

表 4：本阶段工作任务及主要文档

任务	输入文档	任务描述	输出文档
单项测评结果判定	经过测评委托单位确认的测评证据和测评源记录，测评指导书	1.针对每个测评项进行判定； 2.采用“优势证据”法，多结果进行判定	测评报告的单元测评结果记录部分
单元测评结果判定	测评报告的单元测评结果记录部分	按层面分别汇总不同测评对象对应测评指标的单项测评结果情况，包括测评多少项，符合要求的多少项等内容，一般以表格形式列出。	测评报告的单元测评结果汇总和问题分析部分
整体测评	测评报告的单元测评结果记录部分，结果汇总部分和问题	1.针对“部分符合”及“不符合”要求的单个测评项，进行关联关系分析； 2.从安全控制间、层面间和区域间分别进行分析	测评报告的整体测评部分

	分析部分。		
风险分析	填好的调查表格，测评报告的单元测评的结果汇总部分和问题分析部分，测评报告的整体测评部分，测评结果汇总部分。	1.判断整体测评后的部分符合和不符合项所产生的安全问题被威胁利用的可能性； 2.判断整体测评后的部分符合和不符合项所产生的安全问题被威胁利用后对被测信息系统造成的影响程度; 3.结合上述两个方面，进行安全风险赋值； 4.结合被测信息系统的安全保护等级对风险分析结果进行评价	测评报告的风险分析和评价部分
等级测评结论形成	测评报告的测评结果汇总部分，测评报告的风险分析和评价部分	根据测评结果汇总表和风险分析评价表，得出等级测评结论	测评报告的等级测评结论部分
测评报告编制	测评方案，《测评报告模版》，上述各任务的输出文档	编制网络安全等级保护测评报告	经过评审和确认的被测信息系统等级测评报告

1.5 测评技术能力

针对客户单位开展等级测评。依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《信息安全技术信息系统安全等级保护基本要求》（GB/T22239—2019）（以下简称：《基本要求》）中第三级系统的安全要求作为等级测评的基本指标。

第三级系统（S3A3G3）测评要求项指标表

安全层面	数量	控制点
安全物理环境	10	物理位置选择、物理访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

安全通信网络	3	网络架构、通信传输、可信验证
安全区域边界	6	边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证。
安全计算环境	11	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、个人信息保护。
安全管理中心	4	系统管理、审计管理、安全管理、集中管控。
安全管理制度	4	安全策略、管理制度、制定和发布、评审与修订，
安全管理机构	5	岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。
安全管理人员	4	人员录用、人员离岗、安全意识教育培训、外部人员访问管理。
安全建设管理	10	定级和备案、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、工程实施、测试验收、系统交付、等级测评、服务供应商选择
安全运维管理	14	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、外包运维管理。

1.6 测评对象选取

等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合系统的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1）主机房（包括其环境、设备和设施等）；

（2）存储被测系统重要数据的介质的存放环境；

（3）办公场地；

（4）整个系统的网络拓扑结构；

（5）安全设备，包括纵向加密等；

（6）边界网络设备，包括路由器、交换机等；

（7）对整个信息系统或其局部的安全性起作用的网络互联设备，如交换机、路由器等；

（8）承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9）管理终端和主要应用系统终端；

（10）能够完成系统不同业务使命的业务应用系统；

（11）信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（12）涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

1.7 测评方法与工具

本次等级测评的主要方式有：访谈、核查和测试及综合风险分析

●访谈

本次测评采取访谈方式涉及对象为物理安全、网络安全、系统安全、应用安全、数据安全、安全管理等方面内容。其中物理安全、安全管理重点采取访谈方式。在访谈的广度上，访谈覆盖不同类型的系统运维管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等。对测评对象采取抽样的形式确定测评数量；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。测评人员访谈技术负责人、系统管理员、业务开发人员等系统技术架构的实现及配置；访谈系统负责人系统的整体运行状况、安全管理的执行成效。

●检查，包括文档核查及配置核查

本次测评采取检查方式主要涉及对象为物理安全、网络安全、主机系统安全、应用安全、数据安全及安全管理等方面的内容。除物理安全、安全管理主要采取文档核查方式外，其它方面主要采取系统配置核查方式。在核查的广度上，数量

上采取抽样的形式，基本覆盖系统包含的网络设备、安全设备、主机设备、应用软件、管理制度文档等不同类型对象；在核查的深度上，详细分析、观察和研究除了功能级上的文档、机制和活动外，还包括总体/概要和一些详细设计以及实现上的相关信息。

●测试，包括案例验证测试、漏洞扫描测试、渗透性测试。

本次测评采取测试方式主要涉及对象为网络安全、主机系统安全、应用安全、数据安全等方面的内容。其中，案例验证测试主要通过测试工具或案例验证网络安全、应用安全、数据安全的安全功能是否有效。漏洞扫描测试主要分析网络设备、操作系统、数据库等安全漏洞。在核查的广度上，基本覆盖不同类型的机制，在数量、范围上采取抽样方式；在测试的深度上，功能测试涉及机制的功能规范、高级设计和操作规程等文档及深度验证系统的安全机制是否实现，包括冗余机制、备份恢复机制的实现。

●风险分析方法

本项目依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，分析过程包括：

（1） 判断信息系统安全保护能力缺失（等级测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性；

（2） 判断由于安全功能的缺失使得信息系统业务信息安全和系统服务面临的风险；

（3） 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

1.7.1 主要测评工具

工具名称	版本
盛邦一体化漏洞评估系统（RayScan）	Version3.0
Nmap（KALI Linux）	KALI Linux 2022.2
wappalyzer（GOOGLE 插件）	Version-6.10.55
FindSomething（GOOGLE 插件）	Version-2.0.11

FOFA	/
Dirsearch（KALI Linux）	Version-0.43
Xray	Version-1.9.4
Acunetix	Version-15.3
SQLmap（KALI Linux）	Version-1.7
BurpSuit	Version-2022.9
Metasploit（KALI Linux）	Version-6.0.30
Behinder	Version-4.06

1.8 测评强度

测评强度是在测评过程中，对测评内容实施测评的工作强度，体现为测评工作的实际投入程度，反映出测评的广度和深度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多，测评的深度越深，越需要在细节上展开，因此就越需要更多的投入。投入越多就越能为测评提供更好的保证，体现测评强度越强。测评的广度和深度落实到访谈、检查和测试等三种基本测评方式上，其含义有所不同，体现出测评实施过程中访谈、检查和测试的投入程度不同。可以通过测评广度和深度来描述访谈、检查和测试三种测评方式的测评强度。

信息安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，满足相应安全等级的保护要求。测评验证不同安全等级的信息系统是否达具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求，需要实施与其安全等级相适应的测评评估，付出相应的工作投入，达到应有的测评强度。信息安全等级保护要求第一级到第四级信息系统的测评强度在总体上可以反映在访谈、检查和测试等三种基本测评方式的测评广度和深度上，体现在具体的测评实施过程中。

1.9 系统测评实施内容

1.9.1 测评内容与实施

等级测评的现场实施过程由单项测评和整体测评两部分构成。

对应《基本要求》各安全要求项的测评称为单项测评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象

实施的综合安全测评。

通用安全要求

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。 具体分为安全物理环境、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、安全运维管理等方面。

安全物理环境（通用要求）测评指标

序号	安全子类	测评指标描述
1	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；
2		b）机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，否则应加强防水和防潮措施。
3	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
4	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；
5		b）应将通信线缆铺设在隐蔽安全处；
6		c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
7	防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地；
8		b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
9	防火	a）机房应设置火灾自动消防系统，能够自动

序号	安全子类	测评指标描述
		检测火情、自动报警，并自动灭火；
10		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
11		c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
12	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
13		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
14		c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
15	防静电	a）应采用防静电地板或地面，并采用必要的接地防静电措施；
16		b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
17	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
18	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
19		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
20		c）应设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方

序号	安全子类	测评指标描述
		式。
21	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
22	室外控制设备物理防护	a）室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；
23		b）室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

测评实施:安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

安全通信网络（通用要求）测评指标

序号	安全子类	测评指标描述
1	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；
2		b）应保证网络各个部分的带宽满足业务高峰期需要；
3		c）应按照 6.1 节要求的区域划分合理部署系统，带控制功能的系统应部署在生产控制大区的安全区 I 或安全区 II，不带控制功能的系统可部署在管理信息大区，并按照方便管理和控制的原则为各网络区域分配地址；

序号	安全子类	测评指标描述
4		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
5		e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
6	通信传输	a）应采用校验技术或密码技术保证通信过程中数据的完整性，采用密码技术的应按照国家密码管理部门与行业有关要求使用密码算法；
7		b）应采用密码技术保证通信过程中数据的保密性，并按照国家密码管理部门与行业有关要求使用密码算法。
8	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

测评实施:安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的安全保护能力。

安全区域边界（通用要求）测评指标

序号	安全子类	测评指标描述
1	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
2		b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；
3		c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；
4		d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；
5		e）宜采用网络准入、终端控制、身份认证、可信计算等技术手段进行边界安全防护。
6	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
7		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
8		c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
9		d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
10		e）应采用严格的接入控制措施，保证业务系统接入的可信性，经过授权的节点方可接入电力调度数据网；

序号	安全子类	测评指标描述
11		f）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
12	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
13		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
14		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
15		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
16	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
17		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
18	安全审计	a）应在生产控制大区部署专用审计系统，或启用设备或系统审计功能，对网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
19		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
20		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录的留存时间应符合法律法规要求；

序号	安全子类	测评指标描述
21		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
22	拨号使用控制	a）应仅在必要的远程维护时使用拨号认证设施，该设施平时应断电关机，需要时临时开机，使用完毕应及时关机；
23		b）对确需以拨号或 VPN 等方式接入网络的，应仅允许单个用户登录，采用两种或两种以上的认证方式，并对用户访问权限进行严格限制，采取传输加密等措施；
24		c）拨号服务器和客户端均应使用经安全加固的操作系统，并采取数字证书认证、传输加密和访问控制等措施；
25		d）涉及实时控制和数据传输的系统应禁止使用拨号访问服务。
26	无线使用控制	a）应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；
27		b）应对所有参与无线通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；
28		c）应对无线通信采取传输加密的安全措施，实现传输报文的机密性保护；
29		d）对采用无线通信技术进行控制的电力监控系统，应能识别其物理环境中发射的未经授权的无线设备，报告未经授权试图接入或干扰控制系统的

序号	安全子类	测评指标描述
		行为。
30	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

测评实施:安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的网络安全保护能力。

安全计算环境（通用要求）测评指标

序号	安全子类	测评指标描述
1	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，口令长度应不小于 8 位，且为字母、数字和特殊字符的混合组合，账户和口令应不相同，禁止明文存储口令；
2		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
3		c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。
4	访问控制	a）应对登录的用户分配账户和权限；

序号	安全子类	测评指标描述
5		b）应重命名或删除默认账户，修改默认账户的默认口令；
6		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
7		d）应授予管理用户所需的最小权限，实现管理用户的权限分离。
8	安全审计	a）应启用安全审计功能或利用生产控制大区专用审计系统进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
9		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，至少包括用户的添加和删除、审计功能的启用和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；
10		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录的留存时间应符合法律法规要求；
11		d）应对审计进程进行保护，防止未经授权的中断。

序号	安全子类	测评指标描述
12	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
13		b）应关闭不需要的系统服务、默认共享和高危端口，如需使用 SNMP 服务，应采用安全性增强版本，应设定复杂的 Community 控制字段，禁止使用 Public、Private 等默认字段；
14		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
15		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
16		e）应能发现可能存在的已知漏洞，并在经过安全性、兼容性和稳定性等方面充分测试评估后，及时修补漏洞；
17		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
18	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

序号	安全子类	测评指标描述
19	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
20	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。
21	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能，备份数据能够完全恢复至执行时状态，数据保存期限应符合国家相关规定；
22		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
23		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
24	剩余信息保护	应保证操作系统、数据库管理系统、应用系统、中间件、系统管理软件等的鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
25	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；
26		b）应禁止未授权访问和非法使用用户个人信息。

序号	安全子类	测评指标描述
27	控制设备安全	a）控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；
28		b）应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
29		c）应使用专用设备和专用软件对控制设备进行更新；
30		d）应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序；
31		e）应关闭或拆除主机的光盘驱动、USB 接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理。

测评实施:安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在身份鉴别、访问控制、安全审计等方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况）。

安全管理中心（通用要求）测评指标

序号	安全子类	测评指标描述
1	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
2		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等；
3		c）应定期及在配置发生变动前、后分别对设备的配置文件进行备份。
4	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
5		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；
6		c）应严格限制审计数据的访问控制权限，实现审计用户与其他用户的权限分离；
7		d）应定期及在配置发生变动前、后分别对设备的配置文件进行备份。
8	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

序号	安全子类	测评指标描述
9		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等；
10		c）应定期及在配置发生变动前、后分别对设备的配置文件进行备份。
11	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
12		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
13		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
14		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
15		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
16		f）应能对网络中发生的各类安全事件进行识别、报警和分析。

测评实施:安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统的安全保护能力。

安全管理制度（通用要求）测评指标

序号	安全子类	测评指标描述
1	安全策略	应按照“谁主管谁负责，谁运营谁负责”的原则，制定网络安全工作的总体方针和安全策略。阐明机构安全工作的总体目标、范围、原则和安全框架等，并将电力监控系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理。
2	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度，包括：门禁管理、人员管理、权限管理、访问控制管理、防尾随管理、安全防护系统的维护管理、常规设备及各系统的维护管理、恶意代码的防护管理、审计管理、数据及系统的备份管理、个人信息和数据安全管理、用户口令密钥及数字证书的管理、培训管理等；
3		b）需要针对电力监控系统业务需要，如网络安全运维、操作形成专用管理制度；
4		c）应对管理人员或操作人员执行的日常管理操作建立操作规程；
5		d）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
6	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；
7		b）安全管理制度应通过正式、有效的方式发

序号	安全子类	测评指标描述
		布，并进行版本控制。
8	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进、适用环境发生重大变更的安全管理制度，应及时进行修订。

测评实施:安全管理类测评中，技术检测人员将以文档查看和分析为主，访谈为辅获取证据，来评测项目委托单位安全管理类措施的落实情况。安全管理类测评主要涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等。

安全管理机构（通用要求）测评指标

序号	安全子类	测评指标描述
1	岗位设置	a）应明确由主管安全生产的领导作为电力监控系统安全防护的主要责任人，应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
2		b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
3		c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
4	人员配备	a）应配备一定数量的系统管理员、审计管理员和安全管理员等；
5		b）应配备专职安全管理员，不可兼任。
6	授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批；
7		b）应针对系统变更、重要操作、物理访问、系统接入和数据处理等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

序号	安全子类	测评指标描述
8		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
9		d）接入电力调度数据网络的节点、设备和应用系统，其接入技术方案和安全防护措施须经负责管理本级电力调度数据网络的调度机构核准。
10	沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
11		b）应加强与电力监管机构、公安机关、网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
12		c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
13	审核和检查	a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
14		b）应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

序号	安全子类	测评指标描述
15		c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

测评实施:安全管理机构测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等技术检测对象。

安全管理人员（通用要求）测评指标

序号	安全子类	测评指标描述
1	人员录用	a）应指定或授权专门的部门或人员负责人员录用；
2		b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
3		c）应与被录用人员签署保密协议，与系统管理员、审计管理员、安全管理员等关键岗位人员签署岗位责任协议。
4	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
5		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
6	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
7		b）应对安全教育和技能培训的情况和结果进行记录并归档保存，对违反违背安全策略和规定的人员进行惩戒；

序号	安全子类	测评指标描述
8		c）应按照行业要求，对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训，应至少每年举办一次，关键岗位人员的培训内容应包括安全保密教育；
9		d）应定期对不同岗位的人员进行技能考核，考核的结果进行记录并归档保存。
10	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
11		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
12		c）外部人员离场后应及时清除其所有的访问权限；
13		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

测评实施:安全管理人员测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等检测对象。

1.9.2 整体测评

系统整体测评主要是在单项测评的基础上，通过测评分析系统在安全控制间、安全区域间两个方面存在的关联作用验证和分析不符合项是否影响系统的安全保护能力，同时分析系统与其他系统系统边界安全性是否影响系统的安全保护能

力，综合测试分析系统的整体安全性是否合理。系统由于运行环境及系统内部结构的关联性，因此需要针对具体的测评单元间的关联关系分析系统整体安全保护能力。具体内容包括：安全控制间安全测评、区域间安全测评和系统结构安全测评。系统整体测评采取风险分析的方式，由测评中心单独完成。

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对核心业务系统进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。

安全控制间安全测评

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对系统进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。

区域间安全测评

区域间安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。一般边界区域都会和内部某个或某些区域之间发生数据交换；内部不同区域之间也可能因为业务的需要而发生数据交换，需要重点测评这些区域之间的关联作用。

系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。系统结构安全测评的测评范围是整个信息系统，包括被测系统与其他信息系统系统边界之间的安全测评。信息系统整体结构的安全性主要是指从安全的角度，分析信息系统整体结构的安全性（从安全角度看系统）。整体安全防范的合理性主要是指从系统的角度，分析信息系统安全防范的合理性（以系统的观点

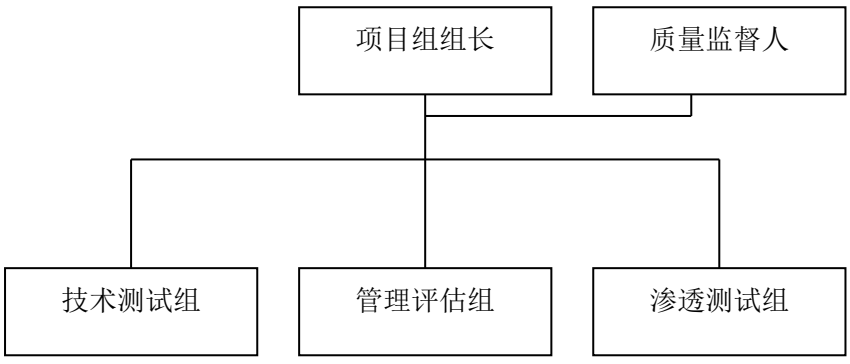
看安全防范（体系））。

从系统整体结构层面分析系统的安全防范能力，对于外部安全威胁的防范主要可以从物理环境保护、系统网络访问控制和系统外联边界控制等几个方面考虑：在物理环境层面上，确保系统所在的中心机房的物理安全和物理访问控制，严格限制非法人员直接进入机房环境或非法设备通过机房环境直接连入系统；在系统网络层面上，保证系统网络访问控制能力，限制设备访问，防范非法设备从内部接入系统；在系统外联边界上，通过各种防护手段（防火墙、路由控制等）和限制外联的通路（只存在与其它可控安全系统的连接，不存在直接接入 Internet 或拨号连出的情况），增强系统的安全保护能力。这几个方面的保护措施相结合，可以对系统进行综合保护，从而确保系统内部安全。整体安全防范的合理性，基于目前部署的安全体系，分析安全设备（如防火墙、防病毒）和安全配置（如访问控制列表）在目前系统中部署是否合理，是否符合成本－效益原则，是否存在重复投资和冗余配置，是否在启用安全措施的同时对系统性能和实际业务需求带来较大负面影响。

1.9.3 项目组织与实施

项目组织

为了保证项目的顺利实施，确保项目质量达到预期目标，将成立项目实施组，以利于加强项目管理和各方面协调合作，使工作和责任更加清晰明确。



项目实施组成员表

项目组组长：负责项目具体实施和管理，制定项目实施计划，掌握项目的每个实施过程，解决项目实施中出现的各种具体问题，项目变化的管理，风险管理，与客户进行及时有效的沟通，定期向用户反馈项目进展情况。

技术测试组：负责项目具体的技术测试实施，如网络平台测试、系统平台测试、业务应用测试等，定期向测评组组长反馈技术测试进展情况。

管理评估组：负责项目具体的安全管理的评估，实施现场访谈、制度核查、执行记录查阅等，定期向测评组组长反馈管理评估进展情况。

渗透测试组：负责汇总技术测试中发现的安全隐患，针对发现的安全漏洞，选择适当的攻击工具及方法，模拟入侵行为。

质量监督人：对项目实施全过程的质量监控，动态监控质量体系执行情况，对违反质量管理规范的情况提出改进或否决意见，及时出具质量监控报告或意见。

进度安排：下表是项目现场实施的工作周期以及各阶段输出结果，具体的项目进度安排计划将由双方在项目启动会议上由双方确认。

系统安全测评项目进度表

实施项目	实施细目	测评周期（天）	备注
一、测评准备过程		5	
现场调查		4	需要系统管理员配合访谈
工具和文档准备		1	
第一阶段输出结果：《测评系统基本情况调查报告》			
二、方案编制过程		5	

实施项目	实施细目	测评周期（天）	备注
方案及计划制定审核		5	
第二阶段输出结果：《系统安全测评方案》、《系统安全测评现场实施计划》			
三、现场实施过程		6	
首次会议	确认方案和计划，协调测评资源	0.5	需要系统方运行相关人员参与
物理安全	机房环境		需要机房管理员配合
网络安全	网络结构分析	0.5	以核查配置文件为主，需要网络管理员配合
	网络设备核查		
	安全设备核查		
主机安全	操作系统核查	1	以核查配置文件

实施项目	实施细目	测评周期（天）	备注
	数据库核查		为主，需要系统管理员配合
	终端设备检查		
应用安全	应用安全核查		核查并验证安全功能的实现，应用系统管理员配合
	应用安全验证测试		
数据安全及备份恢复	数据安全核查分析		需要应用系统管理员或开发人员配合访谈
	数据安全验证测试		
安全管理	安全管理制度	2	需要提供管理文档、执行记录。
	安全管理机构		
	人员安全管理		
	系统建设管理		

实施项目	实施细目	测评周期（天）	备注
	系统运维管理		
漏洞扫描	操作系统、数据库	1	需要系统管理员配合测试
	数据库		
渗透性测试	模拟从 Internet 非授权访问系统	1	需要网络管理员、系统管理员配合测试
测试结果初步分析		1	
末次会议	测评结果交流确认、结果审核		需要系统方运行相关人员参与并确认测评结果
第三阶段输出结果：《系统安全测评记录表》			
四、分析与报告编制过程		10	
测评报告书写		7	

实施项目	实施细目	测评周期（天）	备注
测评报告审核及签发		3	
第四阶段输出结果：《系统安全测评报告》			
总计		26	测评实施阶段工作可根据现场情况并行操作

配合需求

人员配合要求

配合人员列表

配合项目	需求说明
总体协调人	能够进行各种工作的跨部门组织协调的人员
网络管理人员	对系统的网络架构、网络设备、安全设备、管理平台部署情况较为熟悉的人员，现场配合检查组中网络组人员完成网络方面的测评和调研工作。
系统管理人员	对系统中的各类主机的操作系统、数据库系统、各类数据备份等情况较为熟悉的人员，现场配合检查组中主机组人员完成主机和部分数据测评工作。
应用系统开发/运维人员	负责各类应用系统情况、熟悉各类应用在系统中实际部署情况的人员，现场配合检查组中应用组人员完成应用的检查工作。
机房管理人员	负责机房管理的人员，现场配合检查组中管理组完成物理安全测评工作。

配合项目	需求说明
安全文档维护人员	对所有相关的文档进行整理和管理的人员，现场配合检查组中管理组完成管理测评工作。

扫描测试配合要求

扫描测试配合要求列表

配合项目	需求说明
配合人员	网络管理员，提供： 1、（对于每个接入点）可用的以太网电口以及对应的合法 IP 地址； 2、监控网络设备的运行状态。
	主机及业务应用管理员，负责在漏洞扫描期间监控相关主机以及业务应用的运行状态。
安全权限	如接入测评设备时需出入机房，则需要测评人员在测评实施期间出入机房的许可。
	针对 WEB 扫描，需要能够访问目标应用所有应用页面的用户权限。

文档资料配合要求

文档资料配合要求列表

文档名称	具体说明
各类管理制度文档	管理制度、工作单
其他文档	应用系统设计、开发文档

4) 现场工作环境配合要求

相对独立的办公环境，可以容纳 6-8 人左右；

工具测试接入及办公电脑互联网接入；

提供一个保险柜，用于保存工作中的各类过程文档，以防止丢失；

提供一台打印机和打印纸，以便文档的输出。

第四章　投标文件格式

投标文件封面示例

_____（项目名称）

_____项目编号

投标文件

投标人（盖章）：

法定代表人（盖章或签字）：

单位地址：

邮政编码：

联 系 人：

联系电话：

_____年___月___日

目　录

一、投标函
二、资格证明文件索引表
三、商务评审索引表
四、技术评审索引表
五、资格证明文件
1.法定代表人身份证明书
2.法定代表人授权委托书
3.开标一览表（附报价明细表）
4.投标人概况及资质证书
5.具备履行合同所必需的设备和专业技术能力声明函
6.商业信誉和健全的财务制度以及依法缴纳税收和社会保障资金的良好记录
7.参加采购活动前3年内，在经营活动中没有重大违法记录
8、“信用中国”、“中国政府采购网”网站查询企业信用信息截图
9、供应商必须符合法律、行政法规规定的其他条件
10、投标保证金缴纳凭证
11、资格性审查要求的其他资质证明文件
六、商务文件
1、商务条款偏离表
2、企业资质
3、类似业绩
4、人员资质及证书
5、其他商务条款证明材料
七、技术文件
1、技术条款偏离表
2、技术文件
3、测试能力
4、售后服务
5、服务流程
6、额外承诺
八、投标人认为需要提供的其他说明和资料
附件 1：中小企业声明函

自正文粘选目录

注：为了便于查找，请按上述顺序编制投标文件内容，并在目录中标明每项内容的起始页码，电子投标文件中所提供的资料须加盖公章。

一、投标函

投标函

致：

你方组织的（项目名称）（包号）项目的招标[采购项目编号为：_____ _____，我方愿参与投标。

我方确认收到贵方提供的（项目名称）（包号）（项目编号）项目的招标文件的全部内容。

我方在参与投标前已详细研究了招标文件的所有内容，包括澄清、修改文件（如果有）和所有已提供的参考资料以及有关附件，我方完全明白并认为此招标文件没有倾向性，也不存在排斥潜在投标人的内容，我方同意招标文件的相关条款，放弃对招标文件提出误解和质疑的一切权力。

(投标人名称)作为投标人正式授权(授权代表全名,职务)代表我方全权处理有关本投标的一切事宜。

我方已完全明白招标文件的所有条款要求，并申明如下：

（一）按招标文件提供的全部货物与相关服务的投标总价详见《开标一览表》。

（二）本投标文件的有效期为从提交投标（响应）文件的截止之日起 90 日历天。如中标，有效期将延至合同终止日为止。在此提交的资格证明文件均至投标截止日有效，如有在投标有效期内失效的，我方承诺在中标后补齐一切手续，保证所有资格证明文件能在签订采购合同时直至采购合同终止日有效。

（三）我方明白并同意，在规定的开标日之后，投标有效期之内撤回投标或中标后不按规定与采购人签订合同或不提交履约保证金,则贵方将不予退还投标保证金。

（四）我方愿意向贵方提供任何与本项报价有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

（五）我方理解贵方不一定接受最低投标价或任何贵方可能收到的投标。

（六）我方如果中标，将保证履行招标文件及其澄清、修改文件（如果有）中的全部责任和义务，按质、按量、按期完成《采购需求》及《合同书》中的全部任务。

（七）我方作为法律、财务和运作上独立于采购人、采购代理机构的投标人，在此保证所提交的所有文件和全部说明是真实的和正确的。

（八）我方投标报价已包含应向知识产权所有权人支付的所有相关税费，并保证采购人在中国使用我方提供的货物时，如有第三方提出侵犯其知识产权主张的，责任由我方承担。

（九）我方接受采购人委托向贵方支付代理服务费，项目总报价已包含代理服务费，如果被确定为中标供应商，承诺向贵方足额支付。（若采购人支付代理服务费，则此条不适用）

（十）我方与其他投标人不存在单位负责人为同一人或者存在直接控股、管理关系。

（十一）我方承诺未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务。

（十二）我方未被列入法院失信被执行人名单中。

（十三）我方具备《中华人民共和国政府采购法》第二十二条规定的条件，承诺如下：

（1）我方参加本项目政府采购活动前 3 年内在经营活动中没有以下违法记录，或因违法经营被禁止参加政府采购活动的期限已届满：因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚。

（2）我方符合法律、行政法规规定的其他条件。

以上内容如有虚假或与事实不符的，评标委员会可将我方做无效投标处理，我方愿意承担相应的法律责任。

（十四）我方对在本函及投标文件中所作的所有承诺承担法律责任。

（十五）所有与本招标有关的函件请发往下列地址：

地 址：_____邮政编码：_____

电 话：_____

传 真：_____

代表姓名：_____职 务：_____

投标人法定代表人（或法定代表人授权代表）签字或盖章：_____

投标人名称（盖章）：_____

日期： 年 月 日

二、资格证明文件索引表

资格证明文件索引表

请投标人在资格证明文件正文前制作索引表。

序号	评审项目	投标文件位置页码	是否完全响应	
			投标人填写	评委认定
一	资格性审查内容			
1				
2				
3				

二	符合性审查内容			
1				
2				
3				

三、商务评审索引表

商务评审索引表

请投标人在投标书正文前制作索引表。

序号	评审项目	计分模型	标准分值	指标值或评分项	
				投标人填写	投标文件位置页码
	合　计				
一	项目 1				
1	指标 1				
2	指标 2				
3	指标 3				

二	项目 2				
1	指标 1				
2	指标 2				
3	指标 3				

备注：投标人按照《商务评审标准表》编制此表。投标人填写指标值或评分项及其在投标文件位置页码，投标人不得虚报、瞒报、漏报或虚假承诺。

四、技术评审索引表

技术评审索引表

请投标人在投标书正文前制作索引表。

序号	评审项目	计分模型	标准分值	**指标值或评分项**	
				投标人填写	投标文件位置页码
	合　计				
一	项目 1				
1	指标 1				
2	指标 2				
3	指标 3				

备注：投标人按照《技术评审标准表》编制此表。投标人填写指标值或评分项及其在投标文件位置页码，投标人不得虚报、瞒报、漏报或虚假承诺。

五、资格证明文件

1、法定代表人身份证明书

单位名称：

企业类型：

地　　址：

营业期限：

成立时间：

姓名：_____　性别：_____　年龄：_____　职务：

系 _____（投标人名称）_____的法定代表人。

特此证明。

注:附法定代表人身份证正、反面复印件

投标人（盖章）：

日　期：_____年_____月_____日

2、法定代表人授权委托书

本授权委托书声明：我_____（姓名）系_____（投标人名称）的法定代表人，现授权委托_____（投标人名称）的（姓名）为我的代理人，以本公司的名义参加_____（招标人）的招标项目的投标活动。代理人在参加整个项目招标投标活动、合同谈判过程中所签署的一切文件和处理与之有关的一切事物，我均予以承认。

代理人：_____性别：_____年龄：

单　位：_____部门：_____职务：

代理人无转委权。特此委托。

注:附法定代表人及授权委托人身份证正、反面复印件

投标人（盖章）：

法定代表人（盖章或签字）：

日期：_____年____月____日

3、开标一览表

项目名称	
项目编号	
投标总报价（元）	小写： 大写：
服务期限	
备注	

说明：以政采云线上模板为准。

投标单位公章：

法定代表人或法人授权代表（签字或盖章）：

日期：_____年____月____日

附：分项报价报

分项报价表

采购项目编号：

项目名称：

投标人名称：

货币及单位：人民币/元

品目号	类别	名称	范围	要求	期限	单价	数量	总价
1								
2								
…								
合计金额： 人民币小写：￥ 元 人民币大写：元整								

投标人签章：_____

日期：　　年　　月　　日

备注：

1、分项名称和数量应按照第三章“采购需求”内容填写。

2、投标人填报价格合计应与开标一览表载明价格一致。

3、本表中,如未特别注明均是指全部服务范围内的价格构成。

4、投标人概况及资质证书

投标人名称						
注册地址				邮政编码		
联系方式	联系人			电　话		
	传　真			网　址		
组织结构						
法定代表人	姓名		技术职称		电话	
技术负责人	姓名		技术职称		电话	
成立时间			营业执照号			
注册资金			开户银行			
账号						
经营范围						
备注						

备注：投标供应商应附营业执照副本并加盖公章的复印件及本项目特定资格要求所需证书复印件并加盖公章。

附件 1：投标人加盖公章的营业执照复印件；

附件 2：投标人《网络安全等级测评与检测评估机构服务认证证书》。

附件 3：投标人在《商用密码应用安全性评估试点机构目录》中的证明资料。

5、设备及专业技术力量

具备履行合同所必需的设备和专业技术能力声明函

(采购人名称)：

对于贵单位的（项目名称）（包号）（项目编号）采购项目，我公司承诺具备履行合同所必需的设备和专业技术能力。如我单位中标，在项目实施工程中发现声明不实，我单位愿意放弃本次项目的中标资格，并按照《中华人民共和国政府采购法》有关提供虚假材料的规定，接受处罚。

特此声明！

供应商：（签章）

法定代表人或负责人或其委托代理人：（签字或加盖人名章）

日　期：

6、商业信誉和健全的财务制度以及依法缴纳税收和社会保障资金的良好记录

附件 1：供应商必须具有良好的商业信誉和健全的财务会计制度（提供 2023 年度财务状况报告或基本开户行出具的资信证明） 。

附件 2：提供投标截止日前 6 个月内任意 1 个月依法缴纳税收和社会保障资金的相关材料。 如依法免税或不需要缴纳社会保障资金的，提供相应证明材料。

7、参加采购活动前 3 年内，在经营活动中没有重大违法记录

无重大违法记录的书面声明

（采购人）：

在本项目投标文件递交截止时间前，我公司郑重承诺在参加本项目政府采购活动前三年内，在经营活动中无重大违法记录。公司未受到刑事处罚或责令停业、吊销许可证（或执照）、较大数额罚款（较大数额罚款”认定为 200 万元以上的罚款，法律、行政法规以及国务院有关部门明确规定相关领域“较大数额罚款”标准高于 200 万元的，从其规定。）等行政处罚；未处于财产被接管、冻结、破产状况。

如发现我单位提供的声明函不实时，我公司愿意承担一切法律责任并认可采购人或采购代理机构作出的取消中标资格、罚没保证金等决定。

特此声明！

供应商：（公章）

法定代表人或负责人或其委托代理人：（签字或加盖人名章）

日　期：

8、“信用中国”、“中国政府采购网”网站查询企业信用信息截图

附“信用中国”“中国政府采购网”）查询企业信用信息截图（须自招标文件发布之日起至投标文件递交截止时间内从网站中打印）

9、供应商必须符合法律、行政法规规定的其他条件

详见资格评审条款要求

10、投标保证金缴纳凭证

投标人应在此附投标保证金缴纳凭证或电子保函。

11、资格性审查要求的其他资质证明文件

详见资格评审条款要求

六、商务文件

1、商务条款偏离表

项目名称 ：　　项目编号：

序号	条款序号	招标条款	投标条款	备 注

注:若有偏离,请将具体偏离条款在“偏离”一栏中详细说明；若无偏离,请在“偏离”一栏中标注“无”字样。

投标人：_____（单位全称）（盖章）

法定代表人或授权代表_____（签字或盖章）

日　　期：_____年_____月_____日

2、企业资质

详见商务评审条款要求附相关证书及证明材料

3、企业类似业绩

投标供应商应严格按照商务评审要求提供证明材料

企业类似业绩情况表

项目名称	
项目所在地	
发包人名称	
合同价格	
项目描述	
备注	

备注：提供的证明资料以评分标准为准。

投标人：_____（单位全称）（盖章）

法定代表人或授权代表_____（签字或盖章）

4.项目管理机构

投标供应商根据商务评审要求编制、格式自拟（附件相关证书应清晰可辨）。

5、其他商务条款证明材料

未提供格式的商务条款内容或投标供应商认为有必要提供的其它商务证明材料

七、技术文件

1、技术条款偏离表

项目名称 ：　　项目编号：

序 号	条款	项目需求	投标规格	响应/偏离
1				
2				
3				
4				
5				
…				

注:按照第三章采购需求中的技术要求填写，若有偏离,请将具体偏离条款在“偏离”一栏中详细说明；若无偏离,请在“偏离”一栏中标注“响应”字样。

投标人：_____（单位全称）（盖章）

法定代表人或授权代表_____（签字或盖章）

日　　期：_____年_____月_____日

2.技术文件

按照技术评审条款自行拟定技术文件、各项方案、相关证书及证明材料（所附相关证书寄材料应清晰可辨）

（技术文件内容包含：项目总体理解及实施方案；沟通反馈措施、应急、投诉处理方案；服务能力）

3、测试能力

详见技术评审要求，投标供应商根据要求自行编制。

4、售后服务

详见技术评审要求，投标供应商根据要求自行编制。

5.服务流程

详见技术评审要求，投标供应商根据要求自行编制。

6. 额外承诺

详见技术评审要求，投标供应商根据要求自行编制。

八、投标人认为需要提供的其他说明和资料

此部分填报：

1.招标文件未提供格式的内容

2.投标供应商认为有必要提供技术声明及文件资料

3.投标供应商认为有必要提供的其他材料

（内容格式自拟）

附件 1

中小企业声明函（服务业）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔 2020 〕46 号）的规定，本公司（联合体） 参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接）。相关企业的具体情况如下：

1.（标的名称），属于（采购文件中明确的所属行业）；承建（承接） 企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元[1]，属于（中型企业、小型企业、 微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情 形。

本企业对上述声明内容的真实性负责。如有虚假，将依 法承担相应责任。

企业名称（盖章）：

日期：

监狱企业声明函

本公司郑重声明，根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68 号）的规定，本公司为监狱企业。

本公司参加_____单位的_____项目采购活动，采购活动提供本企业（填写制造的货物，由本企业承担工程、提供服务）。

本条所称货物不包括使用大型企业注册商标的货物和服务。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖公章）：

法定代表人或其授权代表(签字)：

日期：

残疾人福利性单位证明材料（残疾人福利性单位参加的）

本单位郑重声明，根据《财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，本单位为符合条件的残疾人福利性单位。

本单位参加（采购代理机构）的（项目名称和采购编号）采购活动，提供本单位的服务。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商（盖章）：

供应商授权代表（签字）：

日　期：