3.1、采购项目概况

根据市卫生健康委安排，近年来我中心承接建设了多个市级卫生健康信息系统并投入使用，部分系统承建商免费运维期限已满。为做好系统运行维护工作，确保系统健康、稳定运行，拟实施2024年市级卫生健康信息系统统一运维服务招标采购。绵阳市全民健康信息平台、电子健康卡管理及应用服务系统、医疗“三监管”平台、诊所在线监管平台等4个系统需每年进行一次三级等保测评，绵阳市互联网+老年健康平台（一期）、公立医院财务监管平台、放射卫生监管平台、继续医学教育管理信息系统等4个系统需每两年进行一次二级等保测评。

3.2、服务内容及服务要求

3.2.1 服务内容

采购包1：
采购包预算金额（元）: 164,200.00
采购包最高限价（元）: 164,200.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	2024 年市级卫生健康信息系统统一运维服务	1.00	164,200.00	套	软件和信息技术服务业	否	否	否	否

采购包2：
采购包预算金额（元）: 480,000.00
采购包最高限价（元）: 440,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	2024 年市级卫生健康信	1.00	440,000.00	套	软件和信	否	否	否	否

	息系统等级保护测评服务				息技术服务业				

3.2.2 服务要求

采购包 1：

标的名称：2024 年市级卫生健康信息系统统一运维服务

参数性质	序号	技术参数与性能指标
★	1	1.服务对象 序号 | 市级卫生健康信息系统名称 1 | 绵阳市检查检验结果互认平台 2 | 绵阳市电子健康卡管理及应用服务系统 3 | 绵阳市医疗“三监管”平台 4 | 绵阳市互联网+老年健康平台一期 5 | 绵阳市病案首页质量管理平台 6 | 绵阳市卫生健康信息化建设项目申报评审管理系统 7 | 绵阳市科研学会质控管理平台 2.服务范围 运维服务范围涵盖上述 7 个系统所涉及的硬件设备、操作系统环境、业务软件系统、数据库系统、接口系统等。包含系统升级与相关软硬件在运行过程中的故障处理、修复、完善、优化、监控及数据整理等服务。 3.服务内容 （1）协助甲方检查系统应用软件运行情况，保障系统功能正常开展，及时排查处理软件故障； （2）负责检查系统前置设备的运行情况，负责处理设备故障； （3）根据甲方提出的数据维护需求，提供相应的数据处理措施，完成诸如核对、恢复、变更、清除、统计等业务数据维护工作； （4）根据甲方提出的数据统计需求，完成后台数据查询提取工作； （5）定期完成数据的备份或迁移维护工作； （6）负责配合因系统功能变更、系统切换所包含的接口调试工作； （7）负责系统功能问题完善，对现存业务功能中出现的数据错误、功能运行异常等系统问题进行修复变更； （8）根据甲方提出的软件维护需求，对应用软件进行效率优化； （9）对甲方提供所需的业务资料、技术资料、软件资料，配合完成相关文档的编写工作；

（10）针对软件版本更新内容完成相关操作手册、培训资料的整理工作，并可根据甲方需求提供一年至少两次的业务用户线上培训；

（11）负责面向业务用户提供线上问题答疑、差错定位及使用指导等工作；

（12）协助完成上级或第三方对系统的审查评估等技术性工作；

（13）协助等保测评单位完成系统的整改工作。

（14）每季度上门回访市卫健委业务科室收集意见。

4.运维服务方式

根据本项目服务要求，提供 7*24 小时的电话、在线以及远程处理等方式的在线答疑、故障排查、故障处理等技术支持服务。当系统平台软硬件出现故障时，服务技术人员在一小时规定时间内进行响应，无法远程解决时，到达现场处理故障，并形成故障登记及处理记录。如发生不可恢复的硬件故障，积极协助甲方寻找备件保障系统及时正常运行。故障分级及响应时间如下表：

故障级别	响应时间	故障解决时间
一级： 属于紧急问题，其具体现象为：系统崩溃导致业务停滞、数据丢失。	15 分钟，1 小时内提交故障处理方案	6 小时以内
二级： 属于严重问题，其具体现象为：客户端、平台、应用系统无法正常登录，影响数据的提交、审核等。	30 分钟，2 小时内提交故障处理方案	12 小时以内
三级： 属于较严重问题，出现系统报错或警告，部分重要功能出现问题，但业务系 统能继续运行且性能不受影响。	30 分钟，4 小时内提交故障处理方案	24 小时以内
四级：	30 分钟，8 小时内提交	48 小时以内

			属于普通问题，其具体现象为：非核心设备问题、系统插件安装，配置咨询或系统操作问题或其他显然不影响业务的问题。	故障处理方案		

采购包 2：

标的名称：2024 年市级卫生健康信息系统等级保护测评服务

<table>
<tr><td>参数性质</td><td>序号</td><td>技术参数与性能指标</td></tr>
<tr><td>★</td><td>1</td><td>按照《中华人民共和国网络安全法》要求“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。”以及《信息安全等级保护管理办法》要求“信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评”。
测评内容包括技术和管理测评：
1. 技术安全性测评包括但不限于：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。
2. 管理安全测评包括但不限于：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。
测评对象及范围
市级卫生健康信息系统，本次等级保护测评系统包括：
<table>
<tr><td>序号</td><td>系统名称</td><td>安全保护等级</td></tr>
<tr><td>1</td><td>绵阳市全民健康信息平台</td><td>S3A3G3（三级）</td></tr>
<tr><td>2</td><td>绵阳市电子健康卡管理及应用服务系统</td><td>S3A3G3（三级）</td></tr>
<tr><td>3</td><td>绵阳市医疗“三监管”平台</td><td>S3A3G3（三级）</td></tr>
<tr><td>4</td><td>绵阳市诊所在线监管平</td><td>S3A3G3（三级）</td></tr>
</table>
</td></tr>
</table>

	台	
5	绵阳市互联网+老年健康平台（一期）	S2A2G2（二级）
6	绵阳市公立医院财务监管平台	S2A2G2（二级）
7	绵阳市放射卫生监管平台	S2A2G2（二级）
8	绵阳市继续医学教育管理信息系统	S2A2G2（二级）

依据标准

①《中华人民共和国网络安全法》

②GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

③GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》

④GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》

⑤GB/T36627-2018《信息安全技术 网络安全等级保护测试评估技术指南》

⑥《信息安全等级保护管理办法》公通字［2007］43 号

⑦《网络安全等级保护测评机构管理办法》公信安［2018］765 号

测评原则

客观性和公正性原则：

虽然测评工作不能完全摆脱个人主张或判断，但测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

经济性和可重用性原则：

基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

可重复性和可再现性原则：

不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

结果完善性原则：

测评所产生的结果应当证明是良好的判断和对测评项的正确理

解。测评过程和结果应当服从正确的测评方法以确保其满足测评项的要求。

项目具体要求

对信息系统安全等级保护状况进行测试评估，应包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

对安全控制测评的描述，使用工作单元方式组织。工作单元分为安全技术和安全管理两大类。安全技术测评包括：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面；安全管理测评包括：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

测评单位根据国家对信息安全等级保护工作的相关法律和技术标准要求，结合本项目的系统保护等级开展实施与之相应的检查、访谈、测试工作。

测评要求

（1）安全物理环境

序号	工作单元名称	工作单元描述
1	物理位置选择	通过访谈、检查机房等信息系统物理场所在位置上是否具有防雷、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈、检查主机房出入口、机房分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	通过访谈、检查机房的主要设备、介质和防盗报警系统等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈、检查机房的设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈、检查机房的设计/验收文档，检查机

				房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
		6	防水和防潮	通过访谈、检查机房的除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
		7	防静电	通过访谈、检查机房是否采取必要措施防止静电的产生。
		8	温湿度控制	通过访谈、检查机房温、湿度情况，是否采取必要措施对机房内的温湿度进行控制。
		9	电力供应	通过访谈、检查机房供电线路、设备等过程，是否具备提供一定的电力供应的能力。
		10	电磁防护	通过访谈、检查是否具备一定的电磁防护能力。

（2）安全通信网络

序号	工作单元名称	工作单元描述
1	网络架构	通过访谈、检查、测试网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络宽带分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性，以及通信线路、关键设备硬件冗余，系统可用性保证情况。
2	通信传输	通过访谈、检查、测试通信传输过程的数据完整性和保密 性保护情况。
3	可信验证	通过访谈、检查通信设备的系统引导、系统程序、重要配置参数和通信应用程序等进行可信验证及应用程序的关键执行环节进行动态可信验证的保护情况。

（3）安全区域边界

序号	工作单元名称	工作单元描述
1	边界防护	通过访谈、检查、测试边界完整性检查设备，测评分析跨域边界的访问控制和数据流通过边界设备的控制措施，非法内联、外联、无线准入控制的监测、阻断等能力。
2	访问控制	通过访谈、检查、测试网络访问控制设备策略部署，测试系统对外暴露安全漏洞情况等过程，测评分析对进出网络的数据流量控制以及基于应

				用协议和应用内容的访问控制能力。
		3	入侵防范	通过访谈、检查、测试网络边界处、关键网络节点检测、防止或限制从内部和外部发起网络攻击行为的防护能力，以及网络行为分析、监测、报警能力，特别是新型网络攻击行为的分析，对攻击行为的检测是否涉及攻击源、攻击类型、攻击目标、攻击事件、入侵报警等方面的防范能力。
		4	恶意代码和防垃圾邮件	通过访谈、检查、测试关键网络节点处对恶意代码、垃圾邮件进行检测、防护和清除、恶意代码防护机制的升级和更新维护等情况
		5	安全审计	通过访谈、检查网络边界、重要网络节点安全审计情况等，测评分析信息系统审计配置和审计记录保护，审计内容等情况。
		6	可信验证	通过访谈、检查边界设备的系统引导、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及应用程序的关键执行环节进行动态可信验证的保护情况。

（4）安全计算环境

序号	工作单元名称	工作单元描述
1	身份鉴别	通过访谈、检查、测试对登录的用户进行身份标识和鉴别，是否具有不易被冒用的特点，口令应有复杂度要求并定期更换，以及远程管理安全、双因素鉴别等内容。
2	访问控制	通过访谈、检查、测试是否启用访问控制功能，依据安全策略控制用户对资源的访问；是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限等内容。
3	安全审计	通过访谈、检查安全审计范围及内容。
4	入侵防范	通过访谈、检查、测试是否能够检测到对重要节点进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警，是否遵循最小化安全装原则、系统服务、默认共享和高危端口、终端接入限制、数据有效性检验、已知漏洞防护等内容。
5	恶意代码防范	通过访谈、检查、测试是否具有防恶意代码攻击的技术措施或主动免疫可信验证机制，能否及时识别入侵和病毒行为并将其有效阻断等内容。

6	可信验证	通过访谈、通过访谈安全员，检查计算设备的系统引导、系统程序、重要配置参数和应用程序等进行可信验证应用程序的关键执行环节进行动态可信验证的保护情况。
7	数据完整性	通过访谈、检查、测试重要数据在传输和存储过程中的完整性保护情况，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
8	数据保密性	通过访谈、检查、测试重要数据在传输和存储过程中的保密性保护情况，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
9	数据备份恢复	通过访谈、检查、测试重要数据本地备份与恢复功能，异地实时备份功能，以及重要数据处理系统的热冗余和高可用性保证等。
10	剩余信息保护	通过访谈、检查、测试边界信息在存储空间被释放或重新分配前是否有效清除，存有敏感数据的存储空间被释放或重新分配前是否有效清除等。
11	个人信息保护	通过访谈、检查、测试是否仅采集和保存业务必须的用户个人信息，对用户个人信息的访问和使用等。

（5）安全管理中心

序号	工作单元名称	工作单元描述
1	系统管理	通过访谈、检查、测试对系统管理员身份鉴别、命令或操作管理、操作审计，以及是否通过系统管理对系统资源和运行进行配置、控制和管理等。
2	审计管理	通过访谈、检查、测试对审计管理员身份鉴别、命令或操作管理、操作审计，以及是否通过审计管理员对审计策略、审计记录进行分析、处理等。
3	安全管理	通过访谈、检查、测试对安全管理员身份鉴别、命令或操作管理、操作审计，以及是否通过安全管理员对安全策略、参数进行配置等。
4	集中管控	通过访谈、检查、测试是否具有特定的管理区域，对分布在网络中的安全设备或安全组件进行集中管控，对网络链路、安全设备、网络设备和服务的运行进行集中监测，对分散在各设备上的审计数据进行收集汇总和集中分析，并确保记录留存符合法律法规要求，对安全策略、恶意代码、

		升级补丁等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析等。	

（6）安全管理制度

序号	工作单元名称	工作单元描述
1	安全策略	通过访谈、检查网络安全工作的总体方针我安全策略是否全面、完善。
2	管理制度	通过访谈、检查管理制度的制定和发布过程是否遵循一定的流程。
3	制度和发布	通过访谈、检查管理制度定期评审和修订情况。
4	评审和修订	通过访谈、检查管理制度在内容覆盖上是否全面、完善。

（7）安全管理机构

序号	工作单元名称	工作单元描述
1	岗位设置	通过访谈、检查安全主管部门设置情况以及各岗位设置和岗位职责情况。
2	人员配备	通过访谈、检查各个岗位人员配备情况。
3	授权和审批	通过访谈、检查对关键活动的授权和审批情况。
4	沟通和合作	通过访谈、检查内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	通过访谈、检查安全工作的审核和检查情况。

（8）安全管理人员

序号	工作单元名称	工作单元描述
1	人员录用	通过访谈、检查录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	通过访谈、检查人员离岗时是否按照一定的手续办理。
3	安全意识教育和培训	通过访谈、检查是否对人员进行安全方面的教育和培训。

		4	外部人员访问管理	通过访谈、检查对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

（9）安全建设管理

序号	工作单元名称	工作单元描述
1	定级和备案	通过访谈、检查是否按照一定要求确定系统的安全等级。
2	安全方案设计	通过访谈、检查整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	通过访谈、检查是否按照一定的要求进行系统的产品采购。
4	自行软件开发	通过访谈、检查自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	通过访谈、检查外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。
6	工程实施	通过访谈、检查建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	通过访谈、检查系统运行前是否对其进行测试验收工作。
8	系统交付	通过访谈、检查是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	通过访谈、检查等级测评、整改情况。
10	服务商选择	通过访谈、检查是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

（10）安全运维管理

序号	工作单元名称	工作单元描述
1	环境管理	通过访谈、检查是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	通过访谈、检查是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	通过访谈、检查是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。

		4	设备维护管理	通过访谈、检查是否采取必要的措施确保设备在使用、维护和销毁等过程安全。
		5	漏洞和风险管理	通过访谈、检查安全漏洞和隐患识别、处理情况，以及是否定期开展安全测评以及安全问题的应对措施。
		6	网络和系统安全管理	通过访谈、检查是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。
		7	恶意代码防范管理	通过访谈、检查是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
		8	配置管理	通过访谈、检查基本配置信息管理情况
		9	密码管理	通过访谈、检查是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
		10	变更管理	通过访谈、检查是否采取必要的措施对系统发生的变更进行有效管理。
		11	备份与恢复管理	通过访谈、检查是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
		12	安全事件处置	通过访谈、检查是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
		13	应急预案管理	通过访谈、检查是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
		14	外包运维管理	通过访谈、检查外包运维服务商选择是否符合国家要求，外包运维保密、服务内容管理等。

（11）安全扩展要求

按照所测评系统的具体情况选用云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求。

（12）验证测试相关要求

按照等级保护测评要求，测评过程中应配备必要的工具、仪器/设备对信息系统进行验证测试，采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。

验证测试内容包括但不限于以下内：

1.渗透测试

验证安全策略正确性；保证用户登录窗体身份验证的安全性；非授权用户不能浏览到未授权内容；不存在跨站点脚本攻击漏洞；脚本不存在 SQL、Cookie 注入漏洞；安全的处理异常，没有出错页面泄露系统信息；应用和系统漏洞及其他，并提出整改建议。验证内容包括（但不限于）以下几个方面：

注入	失效的身份认证
敏感信息泄露	XML 外部实体（XXE）
失效的访问控制	安全配置错误
跨站脚本（XSS）	不安全的反序列化
使用含有已知漏洞的组件	不足的日志记录和监控

2．性能测试

通过模拟手段对网络（包括丢包、时延、带宽等）、软件系统（包括负载、响应）、负载下硬件占用（包含 CPU、内存）等进行全面的测评评估验证系统的可靠性、可用性，通过对测试结果的分析，给出相应的整改建议。

3．漏洞扫描

据相关标准、规范要求对重要信息系统的安全漏洞进行测评。分析总结系统中存在的主要安全漏洞，指出系统中可能被利用的安全漏洞、系统配置错误等缺陷以及相应的安全加固意见、建议。

（13）其他

测评单位在此次等级保护测评工作开展完成后，针对本项目提供一次渗透测试及漏洞扫描服务，并协助委托方对发现的安全问题进行整改。

测评工作步骤

等级保护测评工作流程，受委托测评机构实施的等级测评工作活动及流程与运营、使用单位的自查活动及流程会有所差异，初次等级测评和再次等级测评的工作活动及流程也不完全相同，而且针对不同等级信息系统实施的等级测评工作活动及流程也不相同。受委托测评机构对信息系统的初次等级测评可以分为四项活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评单位应对等级保护测评各阶段具体工作内容进行描述。

1.准备活动阶段：对被测系统进行调研分析，明确测评对象、测评方法等工作。

2.方案编制阶段：制定信息安全等级保护测评项目计划书、测评实施方案，并提交委托方确认。

3.现场测评阶段：按照等级保护相关标准规范要求从访谈、检查、测试几方面进行测试评估并出具《整改意见》，并在整改过程中提供技术咨询服务。

		4.分析与报告编制：向委托方提交被测信息系统安全等级保护测评报告以及相应文档。 **实施要求** 1．系统梳理 协助完成待测信息系统梳理工作。 2．初测 对本项目所涉及信息系统进行现场测评，初次测评完成后提交初评的整改意见报告。 3．整改加固协助 协助对测评过程中发现的安全问题进行技术整改加固工作，并进行整改后的回归测评。 4．成果递交 整理测评结果，提交被测信息系统安全等级保护测评报告以及相应文档。 **项目管理与实施保障** 对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，供应商必须提供完整的项目管理方案，并符合以下要求： 1.供应商及其测评人员应当严格执行有关国家信息安全等级保护相关标准和有关规定，提供客观、公平、公正、有效的等级保护测评服务，并承担相应的法律责任。 2．应具备能够保证其公正性、独立性的质量体系，确保测评活动不受任何可能影响测评结果的商业、财务、健康、环境等方面的压力。 3.供应商在对被测评单位开展等级保护测评服务之前需与被测评单位签订保密协议，测评过程中向被测评单位借阅的文档资料应在测评工作结束后全部归还被测评单位，未经被测评单位允许，不得擅自复制、保留。 4．供应商的岗位配置要至少配置项目经理（或总测评师）、技术负责人、质量负责人、保密安全员和档案管理员，其中项目经理（或总测评师）、技术负责人、质量负责人、保密安全员和档案管理员应独立配置，不能有兼任的情况。 5．测评人员要求 参与此次等级保护测评的供应商其测评人员应具备并符合以下要求： （1）开展此次等级保护测评工作的人员仅限于中华人民共和国境内的中国公民，且无犯罪记录。 （2）开展此次等级保护测评工作的人员应具备从事信息系统安全测评相关工作三年以上工作经验，开展等级保护测评工作不少于一年，参与同类行业信息安全测评项目。 （3）针对软件、网络、云安全等方面的测评技术人员除具有信息安全等级保护测评师证书以外，还应该持有相关技术资格证书。 （4）测评项目组人员在对开展等级保护测评工作之前需签订保密协议。

		6．测评工具要求 （1） 采用的测评工具必须获得正版授权，并在有效期内，不得使用盗版软件。 （2）采用的测评工具在功能、性能等满足使用要求前提下，应优先采用具有国内自主知识产权的同类产品。 （3）采用的测评工具的生产商应为正规厂商，具有一定的研发和服务能力，能够对产品进行持续更新并提供质量和安全保障。 （4）测评机构所使用的测评工具不会对系统产生破坏或负面影响。 7．由于测评工作存在一定的风险，包括但不限于：数据丢失、配置参数丢失、网络中断、服务中断等隐患，供应商应当充分识别测评工作可能带来的风险并告知委托方，委托方应当就测评工作存在潜在风险采取必要措施进行确认后方可开展测评。