**测评服务具体要求**

**一、需求及依据**

信息安全等级保护作为国家信息安全保障的基本制度，在 27 号文件“《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）”和 66 号文件“《关于信息安全等级保护的实施意见》（公通字 [2005] 66 号）”发布后得以确立。2007 年 6 月发布《信息安全等级保护管理办法》（公通字 [2007]43 号），标志着等级保护全面推广实施。2017年《网络安全法》对重要信息系统安全的规定，网络运行者应履行网络安全义务，对重要信息系统进行等级保护测评工作；

**二、测评服务系统概况**

|  |  |  |
| --- | --- | --- |
| 系统名称 | 安全保护等级 | 测评年度 |
| HIS | 二级 | 2024年度 |
| LIS | 二级 | 2024年度 |
| PACS | 二级 | 2024年度 |
| 门户网站 | 二级 | 2024年度 |

**1、成果文档交付**

**供应商应对采购人的四个信息系统分别进行等级保护测评，形成相应的报告。**

**（1）供应商在测评后出具符合标准要求的系统安全等级保护测评书面报告及电子文档1份；**

**三、技术服务要求**

1. **系统备案**

按照《信息安全等级保护管理办法》（公通字[2007]43号）和属地公安机关的要求，协助业主方准备等保备案所需相关资料，并到公安机关完成备案工作。

1. **差距评估**

按照《信息安全技术 网络安全等级保护测评过程指南》（GBT 28449-2018）（以下简称“测评过程指南”）所要求的测评方法，对信息系统进行测评，完成的信息系统安全保护能力是否满足《信息安全技术 网络安全等级保护测评基本要求》（GB/T 22239-2019）（以下简称“基本要求”）进行差距评估。

1. **整改建议**

对差距评估中所发现的安全风险和问题，拟定信息安全等级保护建设整改建议，协助业主方进行拟采购安全设备选型，参与评审信息安全等级保护建设方案，对信息安全等级保护的整改情况进行监督和管理，以及对整改建设完成后的结果进行验证工作。

1. **等级测评**

测评流程

将测评过程指南为测评输入，采取相应的（包括：访谈、检查、测试）测评方法，按照相应的测评规程对测评对象（包括：制度文档、各类设备、安全配置、相关人员）进行相应力度（包括：广度、深度）的单元测评、整体测评，最终得到相应的信息系统等级测评报告。

信息系统等级测评工作共分为四项活动，即测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动

测评方法

【**访谈**】

依据测评技术方案（访谈问题）列表对相关人员进行访谈，获取与安全管理有关的评估证据用于判断特定的安全管理措施是否符合国家相关标准以及委托方的实际需求。

【**检查**】

在物理测评中，测评人员采用文档查阅与分析和现场观察等检查操作来获取测评证据，用于判断目标系统在机房安全方面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在主机安全测评、网络安全测评、应用安全测评和数据安全及备份恢复等方面的测评活动中，测评人员综合采用文档查阅与分析、安全配置核查和网络监听与分析等检查操作来获取测评证据，用于判断目标系统在主机、网络和应用层面采用的特定安全技术措施是否符合国家相关标准以及委托方的实际需求。

在安全管理测评中，测评人员主要采用文档查阅与分析来获取测评证据，用于判断特定的安全管理措施是否符合国家、行业相关标准的要求以及委托方的实际需求。

【**测试**】

在网络安全、主机安全和应用安全等方面的测评活动中，测评人员可以采用手工验证和工具测试等测试操作对特定安全技术措施的有效性进行测试，测试结果用于判断目标系统在网络、主机或应用层面采用的特定技术措施是否符合国家相关标准以及委托方的实际需求，并进一步应用于对目标系统进行安全性整体分析。

**测评指标和测评方法**

1. **安全物理环境**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 物理位置的选择 | 应核查所在建筑物是否具有建筑物抗震设防审批文档；应核查机房是否不存在雨水渗漏； 应核查门窗是否不存在因风导致的尘土严重； 应核查屋顶、墙体、门窗和地面等是否不存在破损开裂；检查机房是否不位于所在建筑物的屋顶或地下室；若机房位于屋顶或地下室，则机房是否采取了防水和防潮措施。 |
| 2 | 物理访问控制 | 检查出入口是否配置电子门禁系统；检查电子门禁系统是否可以鉴别、记录进入的人员信息。 |
| 3 | 防盗窃和防破坏 | 检查机房内设备或主要部件是否固定；检查机房内设备或主要部件上是否设置了明显且不易除去的标记；检查机房内通信线缆是否铺设在桥架或管道中；检查机房内是否配置了防盗报警系统或专人值守的视频监控系统；检查防盗报警系统或视频监控系统是否启用。 |
| 4 | 防雷击 | 检查机房机柜、设施和设备是否有接地措施；检查机房内是否设置防感应雷措施；检查防雷装置是否通过验收或国家有关部门的技术检测。 |
| 5 | 防火 | 检查机房是否设置火灾自动消防系统；检查火灾自动消防系统是否可以自动检测火情、自动报警并自动灭火；检查机房验收文档是否明确相关建筑材料的耐火等级；访谈机房管理员是否进行了区域划分；检查各区域间是否采用了防火措施进行隔离。 |
| 6 | 防水和防潮 | 检查窗户、屋顶和墙壁是否采取了防雨水渗透措施；检查机房内是否采取了防止水蒸气结露的措施；检查机房内是否采取了排泄地下积水，防止地下积水渗透和转移的措施。1.检查机房内是否安装了对水敏感的检测装置；检查防水检测和报警装置是否启用。 |
| 7 | 防静电 | 检查机房内是否安装了防静电地板；检查机房内是否采用了接地防静电措施；检查机房是否配置了防静电设备。 |
| 8 | 温湿度控制 | 检查机房是否配备了专用空调（如：精密空调等）；检查机房内温湿度是否在设备运行所允许的范围内. |
| 9 | 电力供应 | 检查供电线路上是否配置了稳压器和过电压防护设备；检查是否配备了UPS等后备电源系统；检查UPS等后备电源系统是否满足设备在断电情况下的正常运行要求；检查机房内是否设置了冗余或并行的电力电缆为计算机系统供电。 |
| 10 | 电磁防护 | 检查机房内电源线缆和通信线缆是否隔离铺设（如：在不同的桥架中铺设等）；检查机房内是否为关键设备配备了电磁屏蔽装置（如：屏蔽机柜、屏蔽机房）。 |

**配合需求**

|  |  |
| --- | --- |
| **配合内容** | **需求说明** |
| 访谈 | 访谈物理安全负责人 |
| 查看材料 | 提供机房管理制度、机房出入记录，来访人员进入机房的审批记录，查机房和办公场地的设计/验收文档，设备管理制度文档，通信线路布线文档，报警设施的安装测评/验收报告），建筑防雷设计/验收文档，机房防火设计/验收文档，火灾自动报警系统设计/验收文档，防静电设计/验收文档，温湿度控制设计/验收文档，电力供应安全设计/验收文档，建筑防水和防潮设计/验收文档和机房湿度记录，检查和维护记录，电磁防护设计/验收文档等 |
| 实地检查 | 进入机房和系统涉及的办公区域实地检查 |

1. **安全通信网络**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 网络架构 | 检查防火墙、核心路由器、核心交换机、汇聚交换机的CPU、内存使用率（若有监控平台则看峰值情况）；访谈管理员是否出现过因设备性能问题导致的网络瘫痪事件；检查出口、核心交换、桌面接入带宽（检查网络设备、网线是否支持相应带宽）；访谈管理员带宽是否满足业务需求，如果有监控平台或QOS则查看流量峰值。1.访谈管理员是否划分了网段和VLAN；检查划分情况是否与访谈情况相符；根据网段功能，找到对应机器检查是否与设置一致；检查重要网段是否直接与外网或其他区域相连；检查重要网段是否设置有访问控制列表或VLAN。2.应访谈网络管理员，询问是否提供主要网络设备、通信线路的硬件冗余； 应检查主要网络设备、主要通信线路是否采用硬件冗余、软件配置等技术手段提供系统的高可用性。 |
| 2 | 通信传输 | 应核查是否在数据传输过程中使用校验技术或密码技术来保证其完整性；应测试验证密码技术设备或组建是否保证通信过程中数据的完整性；应核查是否在通信过程中采取保密措施，具体采用哪些技术措施；应测试验证在通信过程中是否对数据进行加密。 |
| 3 | 可信计算 | 应核查是否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；应核查是否在应用程序的关键执行环节进行动态可信验证；应测试验证当检测到通信设备的可信性受到破坏后是否进行报警；应测试验证结果是否以审计记录的形式送至安全管理中心。 |

**配合需求**

| **配合内容** | **需求说明** |
| --- | --- |
| 访谈 | 访谈网络管理员和安全员 |
| 查看材料 | 提供网络拓扑图、网络设计/验收文档等 |
| 实地检查 | 查看网管系统、检查设备配置等 |

1. **安全区域边界**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 边界防护 | 应核查在网络边界处是否部署访问控制设备；应核查设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略；应采用其他技术手段（如非法无线网络设备定位、核查设备配置信息等）核查或测试验证是否不存在其他未受控端口进行跨越边界的网络通信； 应核查是否采用技术措施防止非授权设备接入内部网络；应核查所有路由器和交换机等相关设备闲置端口是否均已关闭；应核查是否采用技术措施防止内部用户存在非法外联行为；应核查无线网络的部署方式，是否单独组网后再连接到有线网络；应核查无线网络是否通过受控的边界防护设备接入到内部有线网络。 |
| 2 | 访问控制 | 应核查在网络边界或区域之间是否部署访问控制设备并启用访问控制策略；应核查设备的最后一条访问控制策略是否为禁止所有网络通信；应核查是否不存在多余或无效的访问控制策略；应核查不同的访问控制策略之间的逻辑关系及前后排列顺序是否合理；应核查设备的访问控制策略中是否设定了源地址、目的地址、源端口、目的端口和协议等相关配置参数；应测试验证访问控制策略中设定的相关配置参数是否有效；应核查是否采用会话认证等机制为进出数据流提供明确的允许/拒绝访问的能力；应测试验证是否为进出数据流提供明确的允许/拒绝访问的能力；应核查是否部署访问控制设备并启用访问控制策略；应测试验证设备访问控制策略是否能够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。 |
| 3 | 入侵防范 | 应核查相关系统或组件是否能够检测从外部发起的网络攻击行为；应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；应测试验证相关系统或组件的配置信息或安全策略是否有效；应核查相关系统或组件是否能够检测到从内部发起的网络攻击行为；应核查相关系统或组件的规则库版本或威胁情报库是否已经更新到最新版本；应核查相关系统或组件的配置信息或安全策略是否能够覆盖网络所有关键节点；应测试验证相关系统或组件的配置信息或安全策略是否有效；应核查是否部署相关系统或组件对新型网络攻击进行检测和分析；应测试验证是否对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；检查防护日志内容和报警机制是什么；进行渗透测试或漏洞扫描，查看入侵检测设备能否对攻击进行检测和报警。 |
| 4 | 恶意代码和垃圾邮件防范 | 检查关键节点是否有防毒墙或带防病毒模块的防火墙，运行是否正常，授权是否有效，特征库是否最新；检查关键节点是否部署了防垃圾软件的铲平，运行是否正常，授权是否有效，特征库是否最新。 |
| 5 | 安全审计 | 应核查是否部署了综合安全审计系统或类似功能的系统平台；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行了审计；应核查审计记录信息是否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；检查是否部署有日志服务器对日志进行收集；应核查是否对远程访问用户及互联网访问用户行为单独进行审计分析。 |
| 6 | 可信验证 | 应核查是否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；应核查是否在应用程序的关键执行环节进行动态可信验证；应测试验证当检测到边界设备的可信性受到破坏后是否进行报警；应测试验证结果是否以审计记录的形式送至安全管理中心。 |

**配合需求**

|  |  |
| --- | --- |
| **配合内容** | **需求说明** |
| 访谈 | 访谈网络管理员、安全员和安全审计员 |
| 查看材料 | 提供网络拓扑图、网络设计/验收文档，综合安全审计日志记录，边界完整性检查设备运行日志记录，恶意代码产品运行日志等 |
| 实地检查 | 查看运维系统、检查设备配置、工具接入配合 |

1. **安全计算环境**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 身份鉴别 | 应核查用户在登录时是否采用了身份鉴别措施；应核查用户列表确认用户身份标识是否具有唯一性；应核查用户配置信息或测试验证是否不存在空口令用户；应核查用户鉴别信息是否具有复杂度要求并定期更换；应核查是否配置并启用了登录失败处理功能；应核查是否配置并启用了限制非法登录功能，非法登录达到一定次数后采取特定动作，如账户锁定等；应核查是否配置并启用了登录连接超时及自动退出功能；应核查是否采用加密等安全方式对系统进行远程管理，防止鉴别信息在网络传输过程中被窃听；应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；应核查其中一种鉴别技术是否使用密码技术来实现。 |
| 2 | 访问控制 | 应核查是否为用户分配了账户和权限及相关设置情况；应核查是否已禁用或限制匿名、默认账户的访问权限；应核查是否已经重命名默认账户或默认账户已被删除；应核查是否已修改默认账户的默认口令；应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对应；应测试验证多余的、过期的账户是否被删除或停用；应核查是否进行角色划分；应核查管理用户的权限是否已进行分离；应核查管理用户权限是否为其工作任务所需的最小权限；应核查是否由授权主体（如管理用户）负责配置访问控制策略；应核查授权主体是否依据安全策略配置了主体对客体的访问规则；应测试验证用户是否有可越权访问情形；以不同权限用户登录应用，查看其权限是否受到应用系统的限制（用户可以使用的功能，显示的界面等），以验证系统权限分离功能是否有效；不登录系统，直接输入登录后的页面或需要登录后才能访问的功能页面的url，查看是否可以旁路安全策略；同样，可使用低权限用户访问高权限用户才可访问的页面查看结果；不登录系统，直接输入下载文件的url是否可以下载，如输入http://url/download?name=file是否可以下载文件file；渗透测试或漏洞扫描，查看是否能够旁路访问未授权模块或越权访问；应核查是否对主体、客体设置了安全标记；应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。 |
| 3 | 安全审计 | 应核查是否开启了安全审计功能；应核查安全审计范围是否覆盖到每个用户；应核查是否对重要的用户行为和重要安全事件进行审计。应核查审计记录信息是否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；应核查是否采取了保护措施对审计记录进行保护；应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略；应测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否受到保护。 |
| 4 | 入侵防范 | 应核查是否遵循最小安装原则；应核查是否未安装非必要的组件和应用程序；应核查是否关闭了非必要的系统服务和默认共享；应核查是否不存在非必要的高危端口；应核查配置文件或参数是否对终端接入范围进行限制；应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块；应测试验证是否对人机接口或通信接口输入的内容进行有效性检验；应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞；应核查是否在经过充分测试评估后及时修补漏洞；应访谈并核查是否有入侵检测的措施；应核查在发生严重入侵事件时是否提供报警。 |
| 5 | 恶意代码防范 | 应核查是否安装了防恶意代码软件或相应功能的软件，定期进行升级和更新防恶意代码库；应核查是否采用主动免疫可信验证技术及时识别入侵和病毒行为；应核查当识别入侵和病毒行为时是否将其有效阻断。 |
| 6 | 可信验证 | 应核查是否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；应核查是否在应用程序的关键执行环节进行动态可信验证；应测试验证当检测到计算设备的可信性受到破坏后是否进行报警；应测试验证结果是否以审计记录的形式送至安全管理中心。 |
| 7 | 数据完整性 | 应核查系统设计文档，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在传输过程中是否采用了校验技术或密码技术保证完整性；应测试验证在传输过程中对鉴别数据、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进行篡改，是否能够检测到数据在传输过程中的完整性受到 破坏并能够及时恢复；应核查设计文档，是否采用了校验技术或密码技术保证鉴别数据、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在存储过程中的完整性；应核查是否采用技术措施（如数据安全保护系统等）保证鉴别数据、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在存储过程中的完整性；应测试验证在存储过程中对鉴别数据、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进行篡改，是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。 |
| 8 | 数据备份恢复 | 应核查是否按照备份策略进行本地备份；应核查备份策略设置是否合理、配置是否正确；应核查备份结果是否与备份策略一致；应核查近期恢复测试记录是否能够进行正常的数据恢复；应核查是否提供异地实时备份能，并通过网络将重要配置数据、重要业务数据实 时备份至备份场地；应核查重要数据处理系统（包括边界路由器、边界防火墙、核心交换机、应用服务 器和数据库服务器等）是否采用热冗余方式部署。 |
| 9 | 剩余信息保护 | 应核查相关配置信息或系统设计文档，用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全除；应核查相关配置信息或系统设计文档，敏感数据所在的存储空间被释放或重新分配 给其他用户前是否得到完全清除。 |
| 10 | 个人信息保护 | 应核查采集的用户个人信息是否是业务应用必需的；应核查是否制定了有关用户个人信息保护的管理制度和流程；应核查是否采用技术措施限制对用户个人信息的访问和使用；应核查是否制定了有关用户个人信息保护的管理制度和流程。 |

**配合需求**

| **配合内容** | **需求说明** |
| --- | --- |
| 访谈 | 访谈网络管理员、系统管理员、数据库管理员、安全员和安全审计员等 |
| 查看材料 | 查看安全审计日志记录、恶意代码产品运行日志；提供服务器操作系统文档、数据库管理系统文档、主要服务器操作系统维护/操作手册、主要数据库管理系统维护/操作手册，相关备份记录文件、审计记录等；查看主要应用系统设计/验收文档、操作规程和操作记录、相关审计记录、相关备份、恢复记录等 |
| 实地检查 | 查看网管系统、运维系统、备份系统，检查各类设备配置和日志记录，工具接入配合 |

1. **安全管理中心**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 系统管理 | 应核查是否对系统管理员进行身份鉴别；应核查是否只允许系统管理员通过特定的命令或操作界面进行系统管理操作；应核查是否对系统管理的操作进行审计。应核查是否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、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。 |
| 2 | 审计管理 | 应核查是否对审计管理员进行身份鉴别；应核查是否只允许审计管理员通过特定的命令或操作界面进行安全审计操作；应核查是否对安全审计操作进行审计；应核查是否通过审计管理员对审计记录进行分析，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。 |

**配合需求**

| **配合内容** | **需求说明** |
| --- | --- |
| 访谈 | 访谈系统管理员、网络管理员和安全员 |
| 查看材料 | 查看系统管理和审计管理相关策略文件 |
| 实地检查 | 检查系统管理、审计管理策略的完善性，检查系统管理和审计管理类设备配置 |

1. **安全管理制度**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 安全策略 | 应核查网络安全工作的总体方针和安全策略文件是否明确机构安全工作的总体目 标、范围、原则和各类安全策略。 |
| 2 | 管理制度 | 应核查各项安全管理制度是否覆盖物理、网络、主机系统、数据、应用、建设和运 维等管理内容；应核查是否具有日常管理操作的操作规程，如系统维护手册和用户操作规程等；应核查总体方针策略文件、管理制度和操作规程、记录表单是否全面且具有关联性和一致性。 |
| 3 | 制定和发布 | 应核查否由专门的部门或人员负责制定安全管理制度；应核查制度制定和发布要求管理文档是否说明安全管理制度的制定和发布程序、格式要求 及版本编号等相关内容；应核查安全管理制度的收发登记记录是否通过正式、有效的方式收发，如正式发文、领导 签署和单位盖章等。 |
| 4 | 评审和修订 | 应访谈信息/网络安全主管是否定期对安全管理制度的合理性和适用性进行审定；应核查是否具有安全管理制度的审定或论证记录，如果对制度做过修订，核查是否有修订版本的安全管理制度。 |

**配合需求**

| **配合内容** | **需求说明** |
| --- | --- |
| 访谈 | 访谈安全主管 |
| 查看材料 | 提供，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程，评审记录；制度制定和发布要求管理文档，评审记录，安全管理制度，收发登记记录；安全管理制度列表，评审记录，安全管理制度对应负责人或负责部门的清单 |

1. **安全管理机构**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 岗位设置 | 应访谈信息/网络安全主管是否成立了指导和管理网络安全工作的委员会或领导小组；应核查相关文档是否明确了网络安全工作委员会或领导小组构成情况和相关职责；应核查委员会或领导小组的最高领导是否由单位主管领导担任或由其进行了授权；应访谈信息/网络安全主管是否设立网络安全管理工作的职能部门；应核查部门职责文档是否明确网络安全管理工作的职能部门和各负责人职责；应核查岗位职责文档是否有岗位划分情况和岗位职责；应访谈信息/网络安全主管是否进行了安全管理岗位的划分；应核查岗位职责文档是否明确了各部门及各岗位职责。 |
| 2 | 人员配备 | 应访谈信息/网络安全主管是否配备系统管理员、审计管理员和安全管理员；应核查人员配备文档是否明确各岗位人员配备情况；应核查人员配备文档是否配备了专职安全管理员。 |
| 3 | 授权和审批 | 应核查部门职责文档是否明确各部门审批事项；应核查岗位职责文档是否明确各岗位审批事项；应核查系统变更、重要操作、物理访问和系统接入等事项的操作规范是否明确建立了逐级审批程序；应核查审批记录、操作记录，审批结果是否与相关制度一致；应访谈信息/网络安全主管是否对各类审批事项进行更新；应核查是否具有定期审查审批事项的记录。 |
| 4 | 沟通和合作 | 应访谈信息/网络安全主管是否建立了各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通机制；应核查会议记录是否明确各类管理人员、组织内部机构和网络安全管理部门之间开展了合作与沟通；应访谈信息/网络安全主管是否建立了与网络安全职能部门、各类供应商、业界专家及安 全组织的合作与沟通机制；应核查会议记录是否与网络安全职能部门、各类供应商、业界专家及安全组织开展了合作与沟通；应核查外联单位联系列表是否记录了外联单位名称、合作内容、联系人和联系方式等信息。 |
| 5 | 审核和检查 | 应访谈信息/网络安全主管是否定期进行了常规安全检查；应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况；应访谈信息/网络安全主管是否定期进行了全面安全检查；应核查全面安全检查记录是否包括了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；应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录 。 |

**配合需求**

| **配合内容** | **需求说明** |
| --- | --- |
| 访谈 | 访谈安全主管 |
| 查看材料 | 提供相关审批文件、安全管理某方面的负责人，部门、岗位职责文件，人员配备要求的相关文档及管理人员名单，审批事项列表，审批文档。记录等，安全管理机构会议文件，会议记录，外联单位说明文档 |

1. **安全管理人员**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 人员录用 | 应访谈信息/网络安全主管是否由专门的部门或人员负责人员的录用工作；应核查人员安全管理文档是否说明录用人员应具备的条件（如学历、学位要求，技术人员 应具备的专业技术水平，管理人员应具备的安全管理知识等）；应核查是否具有人员录用时对录用人身份、安全背景、专业资格或资质等进行审查的相关 文档或记录，是否记录审查内容和审查结果等；应核查人员录用时的技能考核文档或记录是否记录考核内容和考核结果等；应核查保密协议是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；应核查岗位安全协议是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。 |
| 2 | 人员离岗 | 应核查是否具有离岗人员终止其访问权限、交还身份证件、软硬件设备等的登记记录；应核查人员离岗的管理文档是否规定了人员调离手续和离岗要求等；应核查是否具有按照离岗程序办理调离手续的记录；应核查保密承诺文档是否有调离人员的签字。 |
| 3 | 安全意识教育和培训 | 应核查安全意识教育及岗位技能培训文档是否明确培训周期、培训方式、培训内容和考核方式等相关内容；应核查安全责任和惩戒措施管理文档或培训文档是否包含具体的安全责任和惩戒措施；应核查安全教育和培训计划文档是否具有不同岗位的培训计划；应核查培训内容是否包含安全基础知识、岗位操作规程等；应核查安全教育和培训记录是否有培训人员、培训内容、培训结果等描述；应核查是否具有针对各岗位人员的技能考核记录。 |
| 4 | 外部人员访问管理 | 应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；应核查外部人员访问重要区域的书面申请文档是否具有批准人允许访问的批准签字等；应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等；应核查外部人员访问管理文档是否明确允许外部人员访问的范围、外部人员进入的条件、外部人员进入的访问控制措施等；应核查外部人员访问重要区域的书面申请文档，是否具有批准人允许访问的批准签字等；应核查外部人员访问重要区域的登记记录是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等；应核查外部人员访问管理文档是否明确外部人员接入受控网络前的申请审批流程；应核查外部人员访问系统的书面申请文档是否明确外部人员的访问权限，是否具有允许访问的批准签字等；应核查外部人员访问系统的登记记录是否记录了外部人员访问的权限、时限、账户等；应核查外部人员访问管理文档是否明确外部人员离开后及时清除其所有访问权限；应核查外部人员访问系统的登记记录是否记录了访问权限清除时间。应核查外部人员访问保密协议是否明确人员的保密义务(如不得进行非授权操作，不得复制信息等）。 |

**配合需求**

| **配合项目** | **需求说明** |
| --- | --- |
| 访谈 | 访谈安全主管、人事负负责人 |
| 查看材料 | 提供人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议，岗位安全协议，审查记录；人员离岗管理文档，保密承诺文档；人员考核记录；安全培训计划，培训记录；第三方人员安全责任合同书或保密协议，第三方人员访问管理文档，访问批准文档，登记记录 |

1. **安全建设管理**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 定级和备案 | 应核查定级文档是否明确保护对象的安全保护等级，是否说明定级的方法和理由；应核查定级结果的论证评审会议记录是否有相关部门和有关安全技术专家对定级结 果的论证意见；应核查定级结果部门审批文档是否有上级主管部门或本单位相关部门的审批意见；应核查是否具有公安机关出具的备案证明文档。 |
| 2 | 安全方案设计 | 应核查安全设计文档是否根据安全保护等级选择安全措施，是否根据安全需求调整安全措施；应核查是否有总体规划和安全设计方案等配套文件，设计方案中应包含密码技术相 关内容；应核查配套文件的论证评审记录或文档是否有相关部门和有关安全技术专家对总体安全规划、安全设计方案等相关配套文件的批准意见和论证意见。 |
| 3 | 产品采购和使用 | 应核查有关网络安全产品是否符合国家的有关规定，如网络安全产品获得了销售许可等；应访谈建设负责人是否采用了密码产品及其相关服务；应核查密码产品与服务的采购和使用是否符合国家密码管理主管部门的要求；应核查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。 |
| 4 | 自行软件开发 | 应访谈建设负责人自主开发软件是否在独立的物理环境中完成编码和调试，与实际运行环境分开；应核查测试数据和结果是否受控使用；应核查软件开发管理制度是否明确软件设计、开发、测试和验收过程的控制方法和 人员行为准则，是否明确哪些开发活动应经过授权和审批；应核查代码编写安全规范是否明确代码安全编写规则； 应核查是否具有软件开发文档和使用指南，并对文档使用进行控制；应核查是否具有软件安全测试报告和代码审计报告，明确软件存在的安全问题及可能存在的恶意代码；应核查对程序资源库的修改、更新、发布进行授权和审批的文档或记录是否有批准人的签字；应访谈建设负责人开发人员是否为专职，是否对开发人员活动进行控制等。 |
| 5 | 外包软件开发 | 应核查是否具有交付前的恶意代码检测报告；应核查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；应访谈建设负责人委托开发单位是否提供软件源代码；应核查软件测试报告是否审查了软件可能存在的后门和隐蔽信道。 |
| 6 | 工程实施 | 应核查是否指定专门部门或人员对工程实施进行进度和质量控制；应核查安全工程实施方案是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等；应核查工程监理报告是否明确了工程进展、时间计划、控制措施等方面内容。 |
| 7 | 测试验收 | 应核查工程测试验收方案是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；应核查测试验收报告是否有相关部门和人员对测试验收报告进行审定的意见；应核查是否具有上线前的安全测试报告，报告应包含密码应用安全性测试相关内容。 |
| 8 | 系统交付 | 应核查交付清单是否说明交付的各类设备、软件、文档等；应核查系统交付技术培训记录是否包括培训内容、培训时间和参与人员等；应核查交付文档是否包括建设过程文档和运行维护文档等，提交的文档是否符合管理规定的要求； |
| 9 | 等级测评 | 应访谈运维负责人本次测评是否为首次，若非首次，是否根据以往测评结果进行相应的安全整改；应核查是否具有以往等级测评报告和安全整改方案；应核查是否有过重大变更或级别发生过变化及是否进行相应的等级测评；应核查是否具有相应情况下的等级测评报告；应核查以往等级测评的测评单位是否具有等级测评机构资质。 |
| 10 | 服务供应商选择 | 应访谈建设负责人选择的安全服务商是否符合国家有关规定；应核查与服务供应商签订的服务合同或安全责任书是否明确了后期的技术支持和服务承诺等内容；应核查是否具有服务供应商定期提交的安全服务报告；应核查是否定期审核评价服务供应商所提供的服务及服务内容变更情况，是否具有服务审核报告；应核查是否具有服务供应商评价审核管理制度，明确针对服务供应商的评价指标、考核内容等。 |

**配合需求**

|  |  |
| --- | --- |
| **配合内容** | **需求说明** |
| 访谈 | 访谈安全主管、系统建设负责人 |
| 查看材料 | 提供系统划分文档，系统定级文档，专家论证文档，系统属性说明文档；总体安全策略文档，安全技术框架，安全管理策略文档，总体建设规划书，详细设计方案，专家论证文档，维护记录；产品采购管理制度，产品选型测评结果记录，候选产品名单审定记录；软件设计相关文档和使用指南，审批文档或记录，文档使用控制记录或软件开发安全协议，软件开发文档，软件培训文档；工程安全建设协议，工程实施方案，工程实施管理制度；系统测评方案，测评记录，测评报告，验收报告，验收测评管理制度；系统交付清单，服务承诺书，系统培训记录，系统交付管理制度；系统备案记录 |

1. **安全运维管理**

|  |  |  |
| --- | --- | --- |
| 序号 | 测评指标 | 测评方法描述 |
| 1 | 环境管理 | 应访谈物理安全负责人是否指定部门和人员负责机房安全管理工作，对机房的出入进行管理、对基础设施（如空调、供配电设备、灭火设备等）进行定期维护；应核查部门或人员岗位职责文档是否明确机房安全的责任部门及人员；应核查机房的出入登记记录是否记录来访人员、来访时间、离开时间、携带物品等信息；应核查机房的基础设施的维护记录是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容；应核查机房安全管理制度是否覆盖物理访问、物品进出和环境安全等方面内容；应核查物理访问、物品进出和环境安全等相关记录是否与制度相符；应核查机房安全管理制度是否明确来访人员的接待区域；应核查办公桌面上等位置是否未随意放置了含有敏感信息的纸档文件和移动介质等。 |
| 2 | 资产管理 | 应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、 重要程度和所处位置等内容；应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施 的选取上是否不同；应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求；应核查资产清单中的设备是否具有相应标识，标识方法是否符合相关要求；应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程 度或用途不同进行分类）；应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。 |
| 3 | 介质管理 | 应访谈资产管理员介质存放环境是否安全，存放环境是否由专人管理；应核查介质管理记录是否记录介质归档、使用和定期盘点等情况；应访谈资产管理员介质在物理传输过程中的人员选择、打包、交付等情况是否进行控制；核查是否对介质的归档和查询等进行登记记录。 |
| 4 | 设备维护管理 | 应访谈设备管理员是否对各类设备、线路指定专人或专门部门进行定期维护；应核查部门或人员岗位职责文档是否明确设备维护管理的责任部门；应核查设备维护管理制度是否明确维护人员的责任、维修和服务的审批、维修过程的监督控制等方面内容；应核查是否留有维修和服务的审批、维修过程等记录，审批、记录内容是否与制度相符；应访谈设备管理员含有重要数据的设备带出工作环境是否有加密措施；应访谈设备管理员对带离机房的设备是否经过审批；应核查是否具有设备带离机房或办公地点的审批记录；应访谈设备管理员含有存储介质的设备在报废或重用前，是否采取措施进行完全清除或被安全覆盖。 |
| 5 | 漏洞和风险管理 | 应核查是否有识别安全漏洞和隐患的安全报告或记录（如漏洞扫描报告、渗透测试报告和 安全通报等）；应核查相关记录是否对发现的漏洞及时进行修补或评估可能的影响后进行修补；应访谈安全管理员是否定期开展安全测评；应核查是否具有安全测评报告；应核查是否具有安全整改应对措施文档。 |
| 6 | 网络和系统安全管理 | 应核查网络和系统安全管理文档，系统管理员是否划分了不同角色，并定义各个角色的责任和权限；应访谈运维负责人是否指定专门的部门或人员进行账户管理；应核查相关审批记录或流程是否对申请账户、建立账户、删除账户等进行控制。应核查网络和系统安全管理制度是否覆盖网络和系统的安全策略、账户管理（用户责任、义务、风险、权限审批、权限分配、账户注销等）、配置文件的生成及备份、变更审批、 授权访问、最小服务、升级与打补丁、审计日志管理、登录设备和系统的口令更新周期等方面；应核查重要设备或系统（如操作系统、数据库、网络设备、安全设备、应用和组件）的配置和操作手册是否明确操作步骤、参数配置等内容； 应核查运维操作日志是否覆盖网络和系统的日常巡检、运行维护、参数的设置和修 改等内容；应访谈网络和系统相关人员是否指定专门部门或人员对日志、监测和报警数据等进行分析统计；应核查是否具有对日志、监测和报警数据等进行分析统计的报告；应访谈网络和系统相关人员调整配置参数结束后是否同步更新配置信库，并核实配置信 息库是否为最新版本；应核查是否具有变更运维的审批记录，如系统连接、安装系统组件或调整配置参数等活动；应核查是否具有变更运维的操作过程记录；应访谈系统管理员使用运维工具结束后是否删除工具中的敏感数据；应核查是否具有运维工具接入系统的审批记录；应核查运维工具的审计日志记录，审计日志是否不可以更改；应访谈系统相关人员日常运维过程中是否存在远程运维，若存在，远程运维结束后是否立 即关闭了接口或通道；应核查开通远程运维的审批记录；应核查针对远程运维的审计日志是否不可以更改；应访谈系统相关人员网络外联连接（如互联网、合作伙伴企业网、上级部门网络等）是否都得到授权与批准；应访谈网络管理员是否定期核查违规联网行为； 3) 应核查是否具有外联授权的记录文件。 |
| 7 | 恶意代码防范管理 | 应访谈运维负责人是否采取培训和告知等方式提升员工的防恶意代码意识；应核查恶意代码防范管理制度是否明确对外来计算机或存储设备接入系统前进行恶意代码检查；若采用可信验证技术，应访谈安全管理员是否未发生过恶意代码攻击事件；若采用防恶意代码产品，应访谈安全管理员是否定期对恶意代码库进行升级，且对升级情况进行记录，对各类防病毒产品上截获的恶意代码是否进行分析并汇总上报，是否未出现过大规模的病毒事件；应核查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告。 |
| 8 | 配置管理 | 应访谈系统管理员是否对基本配置信息进行记录和保存；应访谈配置管理人员基本配置信息改变后是否及时更新基本配置信息库；应核查配置信息的变更流程是否具有相应的申报审批程序。 |
| 9 | 密码管理 | 应访谈安全管理员密码管理过程中是否遵循密码相关的国家标准和行业标准要求；应核查相关产品是否获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书； |
| 10 | 变更管理 | 应核查变更方案是否包含变更类型、变更原因、变更过程、变更前评估等内容；应核查是否具有变更方案评审记录和变更过程记录文档；应核查变更控制的申报、审批程序其是否规定需要申报的变更类型、申报流程、审批部门、 批准人等方面内容；应核查是否具有变更实施过程的记录文档；应访谈运维负责人变更中止或失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；应核查是否具有变更恢复演练记录；应核查变更恢复程序是否规定变更中止或失败后的恢复流程。 |
| 11 | 备份与恢复管理 | 应访谈系统管理员有哪些需定期备份的业务信息、系统数据及软件系统；应核查是否具有定期备份的重要业务信息、系统数据、软件系统的列表或清单；应核查备份与恢复管理制度是否明确备份方式、频度、介质、保存期等内容；应核查备份和恢复的策略文档是否根据数据的重要程度制定相应备份恢复策略和程序等。 |
| 12 | 资产管理 | 应核查资产清单是否包括资产类别（含设备设施、软件、文档等）、资产责任部门、 重要程度和所处位置等内容；应访谈资产管理员是否依据资产的重要程度对资产进行标识，不同类别的资产在管理措施 的选取上是否不同；应核查资产管理制度是否明确资产的标识方法以及不同资产的管理措施要求；应核查资产清单中的设备是否具有相应标识，标识方法是否符合相关要求；应核查信息分类文档是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程 度或用途不同进行分类）；应核查信息资产管理办法是否规定了不同类信息的使用、传输和存储等要求。 |
| 13 | 应急预案管理 | 应核查应急预案框架是否覆盖启动应急预案的条件、应急组织构成、应急资源保障、事后教育和培训等方面；应核查是否具有重要事件的应急预案（如针对机房、系统、网络等各个方面）；应访谈运维负责人是否定期对相关人员进行应急预案培训和演练；应核查应急预案培训记录是否明确培训对象、培训内容、培训结果等；应核查应急预案演练记录是否记录演练时间、主要操作内容、演练结果等； 应核查应急预案修订记录是否定期评估并修订完善等。 |
| 14 | 外包运维管理 | 应访谈运维负责人是否有外包运维服务情况；应访谈运维负责人外包运维服务单位是否符合国家有关规定；应核查外包运维服务协议是否明确约定外包运维的范围和工作内容；应核查与外包运维服务商签订的协议中是否明确其具有等级保护要求的服务能力；应核查外包运维服务协议是否包含可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等内容。 |

**配合需求**

|  |  |
| --- | --- |
| **配合内容** | **需求说明** |
| 访谈 | 访问安全主管、资产管理员 |
| 查看材料 | 提供，机房安全管理制度，办公环境管理文档，设备维护记录，机房进出登记表，机房电子门禁系统及其电子记录；资产清单，资产安全管理制度，信息分类标识文档；介质安全管理制度，各类介质清单；设备审批管理文档，设备操作规程，设备使用管理文档，设施、软硬件维护管理制度，设备维护记录，服务器操作日志，配置文档；网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志；系统安全管理制度，系统审计日志，系统漏洞扫描报告；恶意代码检测记录，恶意代码升级记录，恶意代码分析报告；密码管理制度；变更方案，系统变更申请书，变更管理制度，变更申报和审批程序文档，变更失败恢复程序文档，变更方案评审记录，变更过程记录文档；备份管理文档，备份和恢复策略文档，备份设备操作流程文档，备份和恢复程序文档，备份过程记录文档；安全事件记录分析文档，安全事件报告和处置管理制度，安全事件报告和处理程序文档；应急响应预案文档，应急预案培训记录，应急预案演练记录，应急预案审查记录 |

1. **整体测评**

本部分将对系统的单项测评结果中的不符合项，从安全控制点间、层面间和区域间等方面对单元测评的结果进行验证、分析和整体评价。

安全控制间的安全测评主要考虑同一区域内、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。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

区域间的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。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

**评分办法**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评分因素及权重 | 分值 | 评分标准 | 说明 |
| 一 | 价格 | 30 | 1.经评标委员会评审，通过资格性和符合性审查，且投标报价最低的投标人的投标报价作为评标基准价；  2.投标报价得分=(评标基准价／投标报价)×30 |  |
| 二 | 测评方案响应性 | 10 |  | |
| 1 | 测评方案 | 10 | 1.测评方案中包含测评流程、测评方法、测评指标和配合需求的得5分，未包含完整的得3分，一项未包含的不得分；  2.正确理解网络安全等级测评，测评思路清晰、测评内容完整、测评重点突出，针对每点测评要求项提出完善的测评方法，方法全面、合理，并具有很强的针对性的得5分，较为全面、合理，方法针对性较强得3分，未提供的不得分； |  |
| 三 | 专业人员技术力量 | 37 |  | |
| 1 | 投标人机构技术团队情况 | 12 | 拟派技术负责人1名具有:   1. 信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书； 2. 信息安全测评师； 3. 注册信息安全专业人员（CISP）证书； 4. 网络与信息安全应急人员（管理I级）； 5. 具有市级以上职称改革工作领导小组颁发的高级职称证书； 6. 注册云安全系统认证专家（CCSSP）证书。   以上证书每提供一个得2分，最多得12分。未提供不得分。 | 以上人员提供在职证明，如：社保、劳动合同等 |
| 2 | 15 | 1. 拟派项目经理1名具有：   1、信息安全等级评测师（高级）证书或网络安全等级评测师（高级）证书；   1. 2、网络与信息安全应急人员（管理I级）； 2. 3、信息安全测评师； 3. 4、注册云安全系统认证专家（CCSSP）证书   5、信息安全保障人员（CISAW）（认证方向：应急服务）；  6、计算机软件产品检验员证书；  以上证书每提供一个得2分，最多得12分。未提供不得分。  7、获得过国家信息安全等级保护工作协调小组办公室颁发的个人荣誉证书的得3分。 |
| 3 | 10 | 拟派测试团队人员在具有信息安全等级测评师证书的同时具有以下证书：   1. 网络与信息安全应急人员证书 2. 注册网络安全专业防御人员（NSATP-D）； 3. 信息安全保障人员（CISAW）（认证方向：工控网络安全）； 4. 注册云安全系统认证专家（CCSSP）证书； 5. 计算机技术与软件专业技术资格（信息安全工程师）证书.   以上证书全部具有得10分，缺一个扣2分，扣完为止。 |
| 四 | 商务部分 | 23 |  | |
| 1 | 投标人  业绩 | 6 | 2020年1月1日以来，具有信息安全测评项目案例，每具有1个合同得1分，最多得6分； | 附有效证明文件复印件（加盖投标人公章，原件备查）。 |
| 2 | 投标人机构情况 | 17 | 1、具有ISO9001质量管理体系认证证书, 认证范围包括“评估测试服务”得3分；  2、具有ISO20000信息技术服务管理体系证书, 认证范围包括“评估测试服务”得3分；  3、具有ISO27001信息安全管理体系证书, 认证范围包括“评估测试服务”得3分；  4、投标人具有中国合格评定国家认可委员会颁发的检验机构认可证书（CNAS），认可范围为“信息系统网络安全等级保护测评”的得4分。  5、投标人具有检验检测机构认证证书（检验检测能力范围：软件和信息系统安全等级保护测评等相关内容）的得4分。 |