招标编号：N5100012022002309

四川省人民医院核心系统三级等保评审

采

购

需

求

四川省人民医院

四川中泽盛世招标代理有限公司

共同编制

二〇二二年十月

招标项目服务内容及要求、商务要求

一、项目建设背景

为了落实公安部、网信办和卫健委应用系统安全等级保护要求，进一步增强系统安全防护能力，确保系统安全稳定运行，防止因系统安全事件引发安全事故依据 GB/T 22239-2019 信息安全技术网络安全等级保护基本要求、《信息安全等级保护管理办法》（公通字[2007]43 号）和《中华人民共和国网络安全法》等标准规范，四川省人民医院（以下简称“省医院”）特开展此次等级保护测评工作。

二、项目建设目标

依据国家和行业信息安全的相关标准，全面了解和掌握企业为系统现有安全状况，找出其与《信息系统安全等级保护基本要求》对应级别的差距，及时发现系统存在的安全问题，针对等级保护测评中发现的各种安全风险，测评项目组提出适宜的安全整改建议，最终提交该系统等级保护测评报告。

三、项目建设方案

依据《GB/T28448-2019 信息安全技术 网络安全等级保护测评要求》，按照《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）要求，采取相应的测评方法（包括：访谈、检查、测试），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，对测评发现的风险项进行分析评估，提出合理化整改建议，最终得到相应的信息系统等级测评报告。

四、项目建设依据

此次依据的标准包括但不限于以下内容：

（1）《信息安全等级保护管理办法》（公通字[2007]43 号）

（2）GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》

（3）GB/T 20984-2007：《信息安全技术 信息安全风险评估规范》

（4）GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

（5）GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》

（6）GB 17859-1999：《计算机信息系统 安全保护等级划分准则》

（7）GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》

（8）《中华人民共和国网络安全法》

（9）《四川省卫生健康行业网络安全等级保护工作实施方案》川卫函[2019]11号

五、工作内容及要求

1、测评对象

系统名称	安全等级	单价限价
信息管理系统（HIS）	三级	9 万元/年
实验室管理系统（LIS）	三级	9 万元/年
医学影像学管理系统（PACS）	三级	9 万元/年
电子病历系统（EMR）	三级	9 万元/年
门户网站系统	三级	9 万元/年
基于电子病历的医院信息平台系统	三级	9 万元/年
生殖中心智慧平台	三级	9 万元/年
生殖质量控制平台	三级	9 万元/年

2、测评要求

根据项目需求，为保障信息安全现场测评过程安全可控，明确测评人员职责分配、规范测评人员操作，保障测评结果有效，至少包括以下几个流程：

序号	关键实施阶段	工作要求
1	确定测评范围	明确本次被测评信息系统的范围，包括每个信息系统的范围、信息系统的边界等。
2	获得信息系统的信息	通过调查或查阅资料的方式，了解被测评信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等。
3	确定具体的测评对象	初步确定每个信息系统的被测评对象，包括整体对象，如机房、办公环境、网络等，也包括具体对象，如边界设备、网关设备、服务器设备、工作站、应用系统等。
4	确定测评工作的方法	根据信息系统安全等级情况、系统规模大小等，明确本次测评的方法。
5	制定测评工作计划	制定测评工作计划或方案，说明测评范围、测评对象、工作方法、人员组成、角色职责、时间计划等。
6	实施等级保护测评	实施测评，包括人工检查、工具扫描等方式。
7	项目总结	对测评结果进行总结、汇报

3、测评内容

按照信息系统等级保护测评依据开展测评工作（包括不限于以下项目）

（1）物理安全

物理安全检查主要是了解信息系统的物理安全保障情况。涉及对象为机房。在内容上，物理安全层面测评实施过程涉及的工作单元，具体如下表。

表 1 物理安全测评内容

序号	工作单元名称	工作单元描述
1	物理位置的选择	检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	检查机房出入口等过程，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	检查机房内的主要设备、介质和防盗报警设施等过程，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	检查机房设计/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	检查机房防火方面的安全管理制度，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	检查机房及其除潮设备等过程，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	检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	检查机房的温湿度自动调节系统，测评信息系统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	检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。
10	电磁防护	检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

（2）网络安全

网络设备、网络安全设备以及网络拓扑结构等三大类对象。在内容上，网络安全层面测评过程涉及的工作单元，具体如下表。

表 2 网络安全测评内容

序号	工作单元名称	工作单元描述

1	网络结构安全	检查网络拓扑情况、核查核心交换机、路由器，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。
2	网络访问控制	检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等，测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	网络安全审计	检查核心交换机、路由器等网络互联设备的安全审计情况，测评分析信息系统审计配置和审计记录保护情况。
4	边界完整性检查	检查边界完整性检查设备，测评分析信息系统违规联到外部网络的行为。
5	网络入侵防范	测评分析信息系统对攻击行为的识别和处理情况。
6	恶意代码防范	检查网络防恶意代码产品等过程，测评分析信息系统网络边界和核心网段对病毒等恶意代码的防护情况。
7	网络设备防护	检查交换机、路由器等网络互联设备以及防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、登录失败处理、限制非法登录和登录连接超时等，考察网络设备自身的安全防范情况。

（3）主机安全

主机系统安全检查是为了了解评测目标系统的主机系统安全保障情况。在内容上，主机系统安全层面测评实施过程涉及的工作单元，具体如下表。

表 3 主机安全测评内容

序号	工作单元名称	工作单元描述
1	身份鉴别	检查服务器的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4	入侵防范	检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
5	剩余信息保护	检查服务器鉴别信息的存储空间，被释放或再分配给其他用户前得到完全清除。
6	恶意代码防范	检查服务器的恶意代码防范情况。
7	资源控制	检查服务器对单个用户的登录方式、网络地址范围、会话数量等的限制情况。

（4）应用系统安全

应用系统安全检查是为了了解评测“五险合一”业务应用系统的应用安全保障情况。在内容上，应用安全层面测评实施过程涉及的工作单元，具体如下表。

表 4 应用系统安全测评内容

序号	工作单元名称	工作单元描述
1	身份鉴别	检查应用系统的身份标识与鉴别功能设置和使用配置情况；
		检查应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。
2	访问控制	检查应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。
3	安全审计	检查应用系统的安全审计配置情况，如覆盖范围、记录的项目和内容等；
		检查应用系统安全审计进程和记录的保护情况。
4	剩余信息保护	检查应用系统的剩余信息保护情况，如将用户鉴别信息以及文件、目录和数据库记录等资源所在的存储空间再分配时的处理情况。
5	通信完整性	检查应用系统客户端和服务器端之间的通信完整性保护情况。
6	通信保密性	检查应用系统客户端和服务器端之间的通信保密性保护情况。
7	抗抵赖	检查应用系统对原发方和接收方的抗抵赖实现情况。
8	软件容错	检查应用系统的软件容错能力，如输入输出格式检查、自我状态监控、自我保护、回退等能力。
9	资源控制	检查应用系统的资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。

（5）数据安全及备份恢复

数据安全及备份恢复评估是为了了解评测系统的数据安全及备份恢复保障情况。本次测评重点检查系统的数据在采集、传输、处理和存储过程中的安全及安全备份恢复情况。在内容上，实施过程涉及的工作单元，具体如下表。

表 5 数据安全及备份恢复测评内容

序号	工作单元名称	工作单元描述
1	数据完整性	检查操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。

2	数据保密性	检查操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。
3	安全备份和恢复	检查信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。

（6）安全管理制度

安全管理制度测评是为了了解评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。在内容上，安全管理制度测评实施过程涉及的工作单元，具体如下表。

表 6 安全管理制度测评内容

序号	工作单元名称	工作单元描述
1	管理制度	检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。
2	制定与发布	检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
3	评审和修订	检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。

（7）安全管理机构

安全管理机构测评是为了了解评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。在内容上，安全管理机构测评实施过程涉及的工作单元，具体如下表。

表 7 安全管理机构测评内容

序号	工作单元名称	工作单元描述
1	岗位设置	检查部门/岗位职责文件，测评信息系统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	检查人员名单等文档，测评信息系统各个岗位人员配备情况。
3	授权和审批	检查相关文档，测评信息系统对关键活动的授权和审批情况。
4	沟通与合作	检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核与检查	检查记录文档等过程，测评信息系统安全工作的审核和检查情况。

（8）人员安全管理

人员安全管理测评是为了了解评测人员安全方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。在内容上，人员安全管理测评实施过程涉及的工作单元，具体如下表。

表 8 人员安全管理测评内容

序号	工作单元名称	工作单元描述
1	人员录用	检查人员录用文档等过程，测评信息系统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	检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续办理。
3	人员考核	检查有关考核记录等过程，测评是否对人员进行日常的业务考核和工作审查。
4	安全意识教育和培训	检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。
5	外部人员访问管理	检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

（9）系统建设管理

系统建设管理测评是为了了解评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，系统建设管理测评实施过程涉及的工作单元，具体如下表。

表 9 系统建设管理测评内容

序号	工作单元名称	工作单元描述
1	系统定级	检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。
2	安全方案设计	检查系统安全建设方案等文档，测评系统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	测评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	检查相关软件开发文档等，测评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	检查相关文档，测评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	检查相关文档，测评系统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	检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。
8	系统交付	检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。
9	安全服务商选择	测评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）系统运维管理

系统运维管理测评是为了了解评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。在内容上，系统运维管理测评实施过程涉及的工作单元，具体如下表。

表 10 系统运维管理测评内容

序号	工作单元名称	工作单元描述
1	环境管理	检查机房安全管理制度，机房和办公环境等过程，测评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	检查资产清单，检查系统、网络设备等过程，测评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	检查介质管理记录和各类介质等过程，测评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	设备管理	检查设备使用管理文档和设备操作规程等过程，测评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	监控管理和安全管理中心	测评是否采取必要的措施对重要主机的运行和访问权限进行监控管理。
6	网络安全管理	检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测评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。
7	系统安全管理	检查网络安全管理制度、网络审计日志和网络漏洞扫

		描报告等过程，测评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。
8	恶意代码防范管理	检查恶意代码防范管理文档和恶意代码检测记录等过程，测评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。
9	密码管理	测评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	检查变更方案和变更管理制度等过程，测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份和恢复管理	检查系统备份管理文档和记录等过程，测评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	检查安全事件记录分析文档、安全事件报告和处置管理制度等过程，测评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	检查应急响应预案文档等过程，测评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。

★六、交付产物

包括但不仅限于以下资料：

（1）三级等级测评报告（包含整改建议）。

（2）信息系统网络安全三级等级保护备案证明。

（3）公安机关要求的、其他未列入的相关资料。

★七、商务要求

1、付款方式：

当年验收合格后，采购人接供应商合法票据暨采购人要求的支付文件后 60 日内支付当年测评合同总价款 100%。

2、履约保证金：本项目不收取履约保证金。

3、履约时间：本项目采用一招三年方式采购，合同一年一签，第一年服务时间 2023 年 1 月 1 日-2023 年 12 月 31 日。

4、履约地点：四川省人民医院。

5、验收：

（1）验收交付标准和方法：

1）按国家有关规定以及招标文件的质量要求和技术指标、中标人的投标文件及承诺与合同约定标准进行验收，在公安厅当年规定的时间成功上传至省公安厅等级保护网站备案，公安机关颁发信息系统安全等级保护备案证明视为验收合格；

2）其他未尽事宜按照《财政部关于进一步加 强政府采购需求和履约验收管理的指导意见》(财库〔2016〕205 号)的要求进行验收。

（2）履约验收方案：

1）验收组织方式：自行验收

2）是否邀请本项目的其他供应商：否

3）是否邀请专家：否

4）是否邀请第三方检测机构：否

5）履约验收程序：分期验收

6）履约验收时间：公安机关颁发信息系统安全等级保护备案证明后。

7）技术履约验收内容：招标文件要求、投标文件响应内容及合同约定等内容进行技术验收

8）商务履约验收内容：按投标文件响应商务内容验收。

9）履约验收标准：按国家相关法律、行业标准以及招标文件的质量要求和技术指标、中标人的投标文件及承诺验收。

10）履约验收其他事项：履约验收各条款间有不一致时，按较高标准进行。

注：本章中带“★”为实质性要求，必须满足，否则将作无效投标文件处理。