安全等保测评 2024——等保测评方案要求

一、项目建设背景

为了落实公安部、网信办和卫健局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《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《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，自贡市第四人民医院（以下简称“四医院”）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《GBT 28448-2019 信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019》，按照《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）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：

- 《信息安全等级保护管理办法》（公通字[2007]43 号）
- 《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019
- 《信息安全技术信息系统安全等级保护定级指南》GB/T 22240-2012
- 《信息安全技术信息系统安全等级保护实施指南》GB/T 25058-2010
- 《信息安全技术信息安全风险评估规范》GB/T 20984-2007
- 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019》GB/T 28448-2019
- 《信息安全技术 网络安全等级保护测评过程指南》GB/T 28449-2018
- 《中华人民共和国网络安全法》

五、工作内容及要求

5.1 测评对象

系统名称	安全等级
自贡 120 急救系统	三级
医院信息管理(HIS)系统	三级
实验室管理(LIS)系统	三级
影像管理(PACS)系统	三级
电子病历系统	三级
集成平台系统	三级
互联网医院系统	三级
办公(OA)系统	二级
资源规划管理(HRP)系统	二级

5.2 测评要求

按照网络安全等级保护测评依据开展测评工作（包括不限于以下项目）：

1、安全物理环境

安全物理环境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，安全物理环境层面测评实施过程涉及的工作单元，具体如下表：

表 1 安全物理环境测评内容

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、安全通信网络

安全通信网络检查主要是了解系统的网络架构和通信传输等，涉及对象为防火墙、核心路由器、核心交换机等设备和网络架构。在内容上，安全通信网络层面测评过程涉及的工作单元，具体如下表：

表 2 安全通信网络测评内容

序号	工作单元名称	工作单元描述

1	网络架构	检查核心设备的 CPU 和内存使用率，整个网络带宽是否满足现状，VLAN 划分是否合理，网络架构是否做到设备冗余、链路。
2	通信传输	检查数据在传输过程中的的完整性和保密性措施。
3	可信计算	检查设备是否进行可信验证。

3、安全区域边界

安全区域边界检查主要是了解系统在网络边界的防护措施，涉及对象为防火墙、入侵检测、安全审计等安全设备。在内容上，安全区域边界层面测评实施过程涉及的工作单元，具体如下表：

表 3 安全区域边界测评内容

序号	工作单元名称	工作单元描述
1	边界防护	检查网络边界是否有访问控制设备，访问控制策略是否合理，是否关闭了闲置端口等。
2	访问控制	检查网络中的访问控制策略是否合理、有效。
3	入侵防范	检查网络中是否采用了入侵防范措施，验证该措施是否有效。
4	恶意代码和垃圾邮件防范	检查网络中是否有恶意代码和垃圾邮件防范措施。
5	安全审计	检查网络中是否有综合安全审计措施。
6	可信验证	检查设备是否进行可信验证。

4、安全计算环境

安全计算环境检查主要是了解系统的运行环境是否采取了相关安全措施，涉及对象为网络设备、安全设备、操作系统、数据库、中间件等。在内容上，安全计算环境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	检查所有设备的登录用户是否有身份鉴别措施，是否有复杂度、唯一性等检查。
2	访问控制	检查用户的权限分配情况，默认用户和默认口令使用情况等。
3	安全审计	检查是否开启安全审计功能，是否能审计到每个用户，审计记录是否有保护措施。
4	入侵防范	检查设备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	恶意代码防范	检查设备的恶意代码防范情况。
6	可信验证	检查设备是否进行可信验证。
7	数据完整性	检查系统数据的传输完整性和存储完整性措施。
8	数据保密性	检查系统数据的传输保密性和存储保密性措施。
9	数据备份恢复	检查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。
10	剩余信息保护	检查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。
11	个人信息保护	检查系统对个人信息的采集和使用情况。

5、安全管理中心

安全管理中心检查主要是了解系统在管理、审计等集中管理的情况，涉及对象为综合管理类设备、综合审计类设备等。在内容上，安全管理中心实施过程涉及的工作单元，具体如下表：

表 5 安全管理中心测评内容

序号	工作单元名称	工作单元描述
1	系统管理	检查是否对系统管理员进行统一的身份鉴别，操作审计等。
2	审计管理	检查是否对审计管理员进行统一的身份鉴别，操作审计等。
3	安全管理	检查是否对安全管理员进行统一的身份鉴别，操作审计等。
4	集中管控	检查是否划分独立的安全管理区域，是否对网络中运行的设备进行状态监测、日志审计、安全审计等，是否对补丁、恶意代代码进行统一管理。

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	安全策略	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	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。
3	制定和发布	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。
4	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	沟通和合作	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	审核和检查	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、安全管理人员

安全管理人员测评是为了了解单位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，安全管理人员测评实施过程涉及的工作单元，具体如下表：

表 8 安全管理人员测评内容

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	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。
4	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、安全建设管理

安全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，安全建设管理测评实施过程涉及的工作单元，具体如下表：

表 9 安全建设管理测评内容

序号	工作单元名称	工作单元描述
1	定级和备案	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	等级测评	检查系统之前等级测评的情况，以及之前测评机构的资质等。
10	服务供应商选择	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、安全运维管理

安全运维管理测评是为了了解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，安全运维管理测评实施过程涉及的工作单元，具体如下表：

表 10 安全运维管理测评内容

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	设备维护管理	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	漏洞和风险管理	检查系统对于漏洞和安全隐患风险的管理，是否有报告、记录等文档，是否定期开展安全测评等。
6	网络和系统安全管理	检查系统和网络的安全管理文档，是否明确了角色划分、权限划分，是否覆盖安全策略、账户管理、配置文件的生成及备份、变更审批等内容；检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；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；核查开通远程运维的审批记录，核查针对远程运维的审计日志是否不可以更改等。
7	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。
8	配置管理	检查是否对基本配置信息进行记录和保存，基本配置信息改变后是否及时更新基本配置信息库等。
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	备份与恢复管理	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	资产管理	检查是否有资产清单，清单是否包括资产类别、资产责任部门、重要程度和所处位置等内容；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；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。
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。
14	外包运维管理	检查外包运维服务情况，单位是否符合国家有关规定，协议是否明确约定外包运维的范围和工作内容等。

六、交付产物

包括但不仅限于以下资料：

《网络安全等级保护测评报告》

《网络安全等级保护整改建议》