**福州大学附属省立医院安全运维服务**

# 网络安全运维服务

## 主机系统安全检测服务

### 服务范围

福州大学附属省立医院HIS、LIS、EMR、PACS等13个三级业务系统及其他业务系统主要相关服务器、数据库。

### 服务期限

本次服务期限为自开始服务之日起一年。

### 主机系统漏洞扫描服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对主机系统进行漏洞扫描、端口扫描、弱口令扫描等，覆盖系统的补丁、服务的开放性及安全研究机构发现的系统问题等，发现系统本身存在的安全问题。

### 主机系统安全配置核查服务

每年1次指派专业的安全服务工程师到客户现场，参照等级保护2.0合规性标准，对主机系统进行配置核查，发现主机系统配置存在不合理和不安全的情况，提升客户对主机系统配置的安全意识。结合发现的问题进行及时调整，加强主机系统安全。

### 主机系统后门检查服务

定期每季度1次指派专业的安全服务工程师到客户现场，针对主机系统后门进行检查，检查内容包括：

**1）主机系统后门检查**

主机系统被入侵潜伏后，通常存在隐藏比较深的系统后门（Rootkit），重点发现绕过杀毒软件的系统后门。

**2) 主机系统入侵痕迹检查**

针对主机账号、启动项、进程、网络连接等进行检查。

**3) 主机系统日志分析服务**

根据系统层日志、安全日志、应用层日志以及其他特征发现主机系统的入侵痕迹，避免黑客使用隐藏账户等躲避检查的安全隐患。

### 主机系统安全加固辅导服务

定期每季度1次指派专业的安全服务工程师到客户现场，通过分析主机系统漏洞扫描、安全配置核查、后门检查的结果，明确主机系统当前存在的安全问题，对在检测中发现的主机系统安全问题提供安全加固建议及辅导，协助系统管理员完成主机系统后门清理、漏洞加固和配置加固，提高系统的整体安全性，最大限度消除服务器高风险漏洞，使其符合等级保护的基本要求。

### 中间件安全评估与配置加固建议服务

每年1次指派专业的安全服务工程师到客户现场，针对中间件进行安全合规评估，并提供配置加固建议。

结合工具检测和人工安全审查方式来挖掘Apache/IIS/Tomcat/Weblogic/WebSphere等Web应用服务器（中间件）的脆弱性和安全性问题，主要评估账号、日志、配置等不正确的问题带来的安全威胁，帮助用户及早发现中间件存在的风险，避免造成敏感信息泄漏的后果。

针对Apache/IIS/Tomcat/Weblogic/WebSphere等Web应用服务器（中间件）提供加固建议，包括配置加固与优化建议，最大程度降低中间件本身的漏洞风险、纠正中间件使用中构成安全威胁的错误策略、加强中间件账号、日志、配置等带有安全风险的配置，从整体上提升中间件的安全性。

### 数据库安全评估与配置加固建议服务

每年1次指派专业的安全服务工程师到客户现场，针对数据库进行安全合规评估，并提供配置加固建议。

结合工具检测和人工安全审查方式来挖掘数据库系统的脆弱性和安全性问题，主要评估数据库系统安全漏洞、安全配置不正确带来的安全威胁以及由于数据库系统账号、权限等配置不严谨而产生的安全风险。帮助用户及早发现数据库系统存在的风险，避免造成敏感信息泄漏的后果。

提供数据库安全加固建议，包括最大程度降低数据库系统（SQL Server，Oracle等）本身的漏洞风险、纠正数据库系统使用中构成安全威胁的错误策略、加强数据库系统账号、密钥、权限等带有安全风险的配置，从整体上提升数据库系统的安全性。

### 服务价值与交付成果

通过主机安全检测与加固辅导服务，全面深入地发现主机服务器可能存在的安全风险，及时协助修复主机系统层安全中发现的安全漏洞与隐患，最大限度地防止黑客入侵。保证信息系统有效的防护、稳定、安全的运行。

**交付成果：《主机系统安全检测报告》。**

## 应用安全检测服务

### 服务范围

福州大学附属省立医院互联网医院、门户网站及院内互联网新上线的业务系统。

### 服务期限

本次服务期限为自开始服务之日起一年。

### 互联网网站安全监测服务

**1）可用性监测服务**

针对互联网网站应用提供全年可用性监测服务，可用性监测主要涉及以下指标：网站可用性、网站访问的速度情况、网站响应时间，从而判断互联网网站是否能达到最优、最安全的服务质量。通过的可用性检测服务，从互联网线路远程实时监测目标网站站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现网站无法访问，第一时间通知用户。

**2）合规性监测服务**

远程网页变更监测服务

针对互联网网站应用提供全年远程网页变更监测服务，远程网页变更监测服务在远程对比的基本原理上，增加了两大核心技术，来解决业界恶意变更监控普遍误报率较高的问题。一是内容网页前后模糊匹配技术通过预设值敏感度，作为前后匹配误差的判断标准；二是内容匹配算法，不仅对比网页的变化，而是识别内容，并进行非法库的匹配。例如，扫描发现网页修改中出现了“共产党”，其它部分又出现不和谐词语，系统会计算出一个差值，来进行匹配判断是否为恶意变更行为。这样一方面提升扫描效率，一方面极大降低误报率。一旦发现网站网页异常变更，第一时间通知用户。

网页敏感信息监测服务

针对互联网网站应用提供全年网页敏感信息监测服务，对网站存在的敏感信息进行检测，并且可以检测多种类型的敏感信息，同时，还能够支持自定义导入敏感信息，在自身的敏感词库的基础上，不断丰富敏感词汇。监测工具同时利用百度、谷歌等搜索引擎的强大搜索能力，通过搜索引擎接口提交搜索参数，使页面敏感词检测覆盖面更深更广，从而实现远程实时监测目标站点页面状况，一旦发现页面出现敏感关键词，第一时间通知用户并提供安全参考建议，方便用户及时删除敏感内容，避免事件影响扩散，给自身带来声誉和法律风险。

网页恶意链接监控服务

针对互联网网站应用提供全年恶意链接检测服务，检测网站暗链、桥页等恶意链接以及网页新增链接等。通过监测工具内置的暗链特征库，将远程网页信息抓取到本地，进行特征暗链特征匹配，通过排除信任域名库、IP地址域名、常见隐藏手段等的干扰，并结合暗链关键词库的匹配技术，将目前挂暗链主要目的的搜索引擎关键词，准确匹配出来，从而在有效检测暗链的同时，将误报降到最低限度。一旦发现页面出现网页恶意链接，第一时间通知用户。

**3）安全性检测服务**

网站漏洞扫描检测服务

针对互联网网站应用提供全年网站漏洞扫描检测服务，提供OWASP定义的Web威胁相关的漏洞扫描检测，通过远程的网站漏洞扫描检测，同时有效识别Web2.0以及Flash，保障网站漏洞扫描的全面性。

网站漏洞扫描服务提供广度和深度两种扫描方式，广度优先策略是按照网页内容目录层次深浅来爬行页面，处于较浅目录层次的页面首先被爬行。当同一层次中的页面爬行完毕后，爬虫再深入下一层继续爬行，能有效控制页面的爬行深度，避免遇到一个无穷深层分支时无法结束爬行的问题。

网站钓鱼检测服务

针对互联网网站应用提供全年网站钓鱼检测服务，服务工具通过借助搜索引擎的搜索能力以及网页的模糊匹配技术，通过借助网页关键词，判断搜索关键词而来的网站中，是否出现与本域名不匹配，且相似度高的网站，来判断该网站是否为钓鱼网站，一旦发现将第一时间通知用户。

网页木马检测服务

针对互联网网站应用提供全年网页木马检测服务，检测工具采用业内领先的一体化挂马检测技术，高效、准确的识别网站页面中的恶意代码，从而使网站管理员能够第一时间感知网站的安全状态，及时清除网页木马，避免给用户带来安全威胁，继而影响网站信誉。检测工具采用基于沙箱检测和静态特征库匹配相结合的木马检测技术作为网马检测引擎，提高引擎检测准确性，降低误报率。

弱口令检查服务

针对互联网网站对应主机提供全年弱口令检查服务，检测工具基于调度任务对网站主机进行远程自动扫描，获得所述网站主机诸如：SSH、FTP、ORACLE等服务的弱口令信息，包括：用户名、密码。检测工具通过内置的用户名字典和密码字典以及组合字典，可以进行标准模式破解以及组合模式破解两种扫描方式进行弱口令扫描，扫描一方面同弱口令字典中的弱口令进行匹配，另一方面使用获取到的口令进行模拟登陆验证，从而实现弱口令检查功能，从而有效提高弱口令检测效率。

**4）服务价值与交付成果**

采用安全监测服务平台等检测服务工具对单位的互联网网站提供远程安全监测，用户无需安装任何软件或调整网络架构，由于无需购买和部署设备，因此用户可以在几个小时内将监测服务投入运行，并可以在第一时间获得监测到的网站安全问题，并获得专业的技术指导协助。

**交付成果：《互联网网站安全监测报告》。**

### 应用安全检测服务

**1）应用安全漏洞扫描服务**

定期每季度1次指派专业的安全服务工程师到客户现场，为目标应用提供全方位的安全漏洞及安全隐患检查，从攻击者视角审查目标应用系统的脆弱性状况，包括应用漏洞、应用配置。

**2）应用安全漏洞验证服务**

定期每季度1次指派专业的安全服务工程师到客户现场，对已经发现的安全问题进行人工验证，以判断应用当前的漏洞是否真实有利用，剔除误报干扰。并提供专业的安全加固措施指导建议，帮助客户解决当前应用存在的安全问题。

**3）应用安全漏洞加固辅导服务**

定期每季度1次指派专业的安全服务工程师到客户现场，提供专业的应用安全漏洞加固措施指导建议，协助应用开发商及时采取可行的应用安全加固措施进行安全加固。首次安全加固后，将进行漏洞复查和对比，以形成加固前后对比。协助客户解决当前应用存在的安全问题。

**4）服务价值与交付成果**

通过应用安全检测服务，全面深入地挖掘可能存在的被黑客利用的网站应用层安全漏洞和数据库的安全隐患，同时实现对单位作为业主或其负责运维的信息系统在发现漏洞时的有序管理，实现安全事件可追踪、可追溯，保障漏洞得到及时、有效的修复，确保各信息系统的安全运行。

**交付成果：《应用安全检测报告》。**

## 应用系统上线测试服务

### 开放服务安全性评估服务

 通过端口扫描工具检查新系统是否开放了不必要的端口及服务。避免黑客利用不安全的端口及服务进行相关的网络攻击。

### 应用软件安全评估服务

对预上线应用提供软件安全评估服务，查找软件系统安全脆弱性，为软件安全性提供评价。全面检测应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁，漏洞测试覆盖OWASP十大漏洞及上线安全测试标准，如目录遍历漏洞、关键会话重放攻击、任意用户注册、越权访问漏洞、明文传输、SQL注入漏洞、XSS漏洞、上传漏洞、后台泄露漏洞、敏感信息泄露、命令执行等多方面开展软件安全测试。

### 应用安全加固建议及辅导服务

针对软件安全评估及安全配置评估结果，提供应用安全加固建议，并与开发人员和系统建设人员及时沟通，从开发、集成角度提供加固建议，协助开发集成人员修复软件安全风险。

### 服务价值与交付成果

通过Web应用上线测试安全服务来最大程度地发现业务应用系统存在的薄弱环节和安全风险，并通过安全加固修复已知脆弱性，使风险降低到可接受的程度，保证应用系统的可用性、安全性。

**交付成果：《应用系统上线测试报告》。**

## 安全渗透测试服务

### 服务范围

福州大学附属省立医院HIS、LIS、EMR、PACS等13个三级业务系统及其他业务系统。

### 服务期限

本次服务期限为自开始服务之日起一年。

### 网站安全渗透测试服务

每年一次（按需提供不超过三次复查）安排渗透测试团队采用人工黑盒的方式对用户的应用系统进行模拟攻击测试。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、Web脚本渗透、B/S或C/S应用程序测试等，渗透结果进行人工分析，并对漏洞提交源代码加固建议报告。

### 应用安全渗透测试服务

每年一次针（按需提供不超过三次复查）对应用系统进行专家级人工的渗透测试服务，全面检测Web应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁，漏洞测试覆盖OWASP十大漏洞，如XSS跨站脚本攻击漏洞、SQL注入漏洞、恶意代码上传漏洞、Cookie注入漏洞及其它各种敏感信息的检查等。

### 安全加固建议及辅导服务

根据渗透测试结果，提供详细的应用安全加固建议，并协助应用开发公司完成应用加固，并提供复查以确保漏洞得到修复。

### 服务价值与交付成果

（1）深度挖掘应用系统中的安全漏洞，并判断漏洞可能造成的最大限度的损失；

（2）以最权威的客户数据，让客户感受应用系统安全漏洞将带来的影响和损失，以便做好安全损失与保护的评估。

**交付成果：《安全渗透测试报告》。**

## 综合应急安全保障服务

### 安全应急演练服务

**1）应用应急预案设计服务**

针对单位自身的网络实际情况，并结合网络安全应急处置相关的政策要求，设计出1份符合单位要求的安全应急预案，预案中包括5个场景。

制定应急预案管理的责任部门，建立统一的应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；在应急预案框架制定不同事件的应急预案，应急预案要指名适用的系统、设备等，要结合系统实际状况。比如针对门户网站的网页篡改、针对业务系统的入侵等。组织信息网络应急保障队伍，并定期开展应急演练，做好应急演练相关文档记录。

**2）应用应急演练服务**

为保障网络与信息系统安全，预防和遏制网站及应用系统突发安全事件的发生，减轻和消除突发事件造成的危害和影响，组织技术力量共同完成安全应急预案中1个场景的演练，演练完成后提交《应急演练报告》及相关应急演练记录，确保能够应对各类安全事件的发生。

**3）服务价值与交付成果**

通过开展安全应急演练，提高单位对安全突发事件的组织指挥能力和应急处置能力。

**交付成果：《安全应急预案》、《安全应急演练报告》。**

### 安全应急响应服务

**1）安全应急响应服务**

当单位网络和信息系统遇到黑客攻击或网页篡改等恶性事件，迅速对事件做出相应的判断，确认事件给信息系统带来的影响和损害程度，区分一般事件和应急响应事件等，如果确认事件为应急响应事件且远程支持无法解决时，安排工程师到达现场处置，实施最有效的紧急救援及恢复补救方案。

**2）安全应急处置服务**

根据突发事件信息，初步判定突发事件的程度。能够自行解决，要及时加以解决；如果不能自行解决故障，由单位领导现场指挥，协调各部门力量，按照分工负责的原则，组织相关技术人员立即启动应急预案，进入应急预案的处置程序，及时控制安全事件的蔓延，采取有效的措施以防止事件进一步扩大，尽可能地减少负面影响。

**3）远程安全咨询服务**

当单位网络和信息系统故障或出现安全事件时能立即通过电话咨询或远程维护等方式提供7×24小时远程安全咨询服务支持。

**4）服务价值与交付成果**

通过应急响应为遇到黑客攻击或网页篡改等恶性事件，实施最有效的紧急救援及恢复补救工作。

**交付成果：发生安全事件应急响应后提交《安全应急响应报告》。**

### 安全检查专题服务

**1）安全检查专题服务**

在上级监管部门对单位进行安全检查期间，协助单位按照上级监管部门要求，进行专门的全面安全检查协助服务和保障协助，包括协助单位梳理出单位现有的信息安全管理制度相关材料等。

**2）服务价值与交付成果**

通过安全检查专题服务，保障了在上级监管部门安全检查期间能够进行高效的协助工作。

**交付成果：安全检查相关材料。**

### 重保服务

服务期限内，提供护网防守保障服务，主要内容包含护网前期安全风险自查工作、安全整改加固、护网期间监测保障、人员现场值守、护网期间溯源分析、护网期间应急处置、演练后汇报总结服务，并提交防守保障报告。

（1）安全风险自查服务，自查工作内容包含资产梳理、网络架构安全评估、安全策略有效性排查、口令审计及漏洞扫描、互渗透测试、服务器入侵清查、渗透测、基线配置核查、主机安全防护情况排查、目标系统、重要系统区域隔离情况排查等。

（2）安全整改加固服务，整改加固包含强口令、外部访问权限、内部访问IP、业务系统所在网络区域优化、访问控制策略优化，协助进行应用系统漏洞验证和整改。

（3）安全监测保障服务，通过现有的安全监测相关工具结合安全专家团队在客户现场，安全监测分析，对网络中异常流量进行检测分析，及时发现可疑的执行文件和网络流量，针对潜在的未知攻击进行预警。要求护网期间将采用安全监测工具，能够监控黑客入侵过程中修改系统账号、创建敏感文件、植入Rootkit后门等行为。投标时提供功能演示，要求通过模拟黑客利用系统漏洞，向被监控的应用系统主机添加隐藏账号(例如：hack$)，主机安全监控系统应能在1分钟内生成相关的告警，并能够查看告警信息和对应的黑客添加的系统账号名称。

（4）溯源分析服务，派工程师在现场保障值守，现场工程师对监测发现的网络风险、主机风险、网站风险进行统筹溯源分析，对流量日志、主机日志、应用日志进行分析、审计、溯源等操作，找出事件根源所在。

（5）应急处置服务，根据攻击信息，对正在发生或者已经发生的安全事件加以处理，及时修复漏洞、复查漏洞、整改问题，控制安全事件的进一步扩大，确保系统的安全、可靠运行。

（6）汇报总结，对防守过程事宜进行各方协调、汇报工作；撰写总结报告；推进整改问题和复查漏洞。

（7）同时提供全国两会等重要时期保障服务，服务期限内，需在具有重大政治时期加强网络安全保障力度，加强重要网站监测，防范重大网络安全事件的发生，保证医院信息系统的安全稳定运行。投标人提供项目人员为专业团队，且需参与现场保障支持，对威胁告警事件进行分析处置，投标人需定期输出安全值守保障报告并向安全保障指挥领导小组汇报。包括但不限于专家现场安全保障服务、高级攻击诱捕服务、高级威胁情报研判获取服务、攻击预警阻断服务、应急响应处置服务及攻击追溯溯源服务。

### 安全通告服务

**1）安全通告服务**

提供最新的安全动态、技术和安全信息，包括实时安全漏洞通知、定期安全通告汇总和安全知识库更新等。通告内容包括但不限于以下内容：

国内外最新重大漏洞、病毒安全通告；

国家安全政策及法律法规；

同行业安全威胁事件通告；

国内外重大安全事件，新技术发展动态通告；

重大安全漏洞爆发时需结合资产情况，提出相应修复建议。

**2）服务价值与交付成果**

可以根据通告信息，轻松掌握最新的安全漏洞状态并能够安排及时修补IT资产漏洞，提高单位安全脆弱性管理能力。

**交付成果：《安全通告》全年不少于6期。**

## 安全培训服务

### 安全意识培训服务

（1）安全技术培训服务，提供1个课时的安全技术培训，时长45分钟，培训内容包括但不限于以下方面：网站安全防护与维护、网站安全开发、应急响应、等保安全建设、网络安全技术攻防等培训。
 （2）安全意识培训服务，提供1个课时的安全意识培训，时长45分钟，培训内容从个人电脑安全、邮件安全、移动安全、日常工作生活等维度进行强化参训人员的安全意识培训。

### 服务价值与交付成果

通过安全培训服务和安全意识培训服务以满足单位客户获取安全知识和经验的需求，从而使客户最终达到强化安全意识，理解安全理论，掌握安全技术，获得安全实践经验，通过安全认证，能够融会贯通并应用于所在单位的信息化安全建设当中。

**交付成果：安全培训材料。**

## 安全措施有效性验证服务

### 服务范围

福州大学附属省立医院本地相关安全设备。

### 服务期限

本次服务期限为自开始服务之日起一年。

### 网络边界管控有效性及策略核查服务

定期每季度1次指派专业的安全服务工程师到客户现场，对网络边界、外联线路等安全情况进行分析，发现其可能存在的安全隐患。

### 安全设备措施有效性及策略核查服务

定期每季度1次指派专业的安全服务工程师到客户现场，对单位安全设备措施有效性及策略进行核查。

针对防火墙、入侵检测、防病毒网关等安全设备提供以下服务：

1. **安全策略优化：**根据业务变化情况，检查访问控制策略，调整和优化安全规则达到一致性。
2. **运行状态巡检**：检查设备运行状态，性能处理能力是否存在瓶颈或运行异常。
3. **自身安全性检查：**从设备账号管理、远程管理、权限管理等方面开展设备自身安全性检查。
4. **日志巡检：**定期检查相关安全设备日志进行分析，查看是否存在安全隐患。

### 安全软件措施有效性及策略核查服务

定期每季度1次指派专业的安全服务工程师到客户现场，对单位安全软件措施有效性及策略进行核查。

针对网页防篡改、终端防病毒、终端安全管理等现有安全软件提供以下服务：

1. **安全策略优化：**根据业务变化情况，检查访问控制策略，调整和优化安全规则达到一致性。
2. **运行状态巡检：**检查软件运行状态，性能处理能力是否存在瓶颈或运行异常。
3. **自身安全性检查：**从软件账号管理、远程管理、权限管理等方面开展设备自身安全性检查。
4. **日志巡检：**定期检查相关安全软件日志进行分析，查看是否存在安全隐患。

### 服务价值与交付成果

根据业务环境变化情况，定期评估安全设备、安全软件的防护有效性，对已采取的安全措施的有效性进行确认，对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于不适当的安全措施进行优化配置，并定期分析设备告警情况，及时发现安全隐患。

**交付成果：《安全措施有效性验证报告》。**

## 安全设备策略维护服务

### 服务范围

福州大学附属省立医院本地相关安全设备。

### 服务期限

本次服务期限为自开始服务之日起一年。

### 实时策略调整

根据业务变化情况（如新增应用、网络结构调整等），提供安全策略的动态更新支持。此过程包括对防火墙、堡垒机、网闸等多种设备进行配置调整，确保安全策略与网络拓扑结构及业务逻辑保持一致性和匹配性。

根据业务需求，及时响应紧急策略调整需求，例如临时开放特定端口、阻断恶意IP地址等，以应对突发的安全威胁和挑战。

### 定期策略备份

定期执行关键安全设备配置及策略文件的备份工作，以便在设备发生故障或因误操作导致配置丢失时，能够迅速且准确地恢复至先前的配置状态，从而确保业务的连续性和安全性。

**交付成果：**关键安全设备策略备份文件、策略更新调整表（如有）。

# 网络安全等保咨询服务

## 服务周期

本次服务期限为自合同签订生效之日至备案系统通过测评，或一年，以先到为止。

## 服务范围

根据国家、地方、行业的等级保护相关政策和标准要求，分析等级保护对象的具体情况，协助完成HIS、LIS、EMR、PACS等13个三级业务系统，以及≥6个二级信息系统的风险分析、差距分析、整改加固、安全管理制度完善、测评现场辅助的工作,并配合通过网络安全等级保护测评。

## 等保资产分析服务

投标人根据等级保护范围内的资产组成，对服务范围内各个测评对象整理的网络结构拓扑以及相关联的资产，基于等级保护综合管理系统开展安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及安全管理制度进行调研和梳理，编制《信息系统等级保护基本情况调研表》，并通过系统实现资产管理，包含网络拓扑、机房管理、设备管理、应用管理、数据管理等。

## 等保风险分析服务

投标人根据等级保护基本要求，开展安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心的现状分析，通过安全访谈、脆弱性评估、登录检查、日志分析、等级保护综合管理系统等技术手段对现有的安全资产进行全方位的风险评估，结合信息资产属性、威胁、脆弱性等基本要素，分析信息系统安全风险评估分析，编制《等级保护安全评估与整改建议报告》。

## 等保差距评估服务

投标人在安全评估和信息系统定级的基础上，根据《GB/T22239-2019信息安全技术网络安全等级保护基本要求》将测评对象对应等级的等级保护的各项基本要求与信息安全现状进行比较分析，并通过等级保护综合管理系统提供展示本单位的指标自评的总体情况、10大层面指标符合情况、自评得分变化趋势。差距评估从管理和技术两个层面找出存在的问题并进行差距分析，包含以下内容：

安全通用要求差距

**1) 技术层面的差距评估（三级）内容：**

* 安全物理环境：物理位置选择、物理访问控制、防盗窃和防破坏、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：网络架构、通信传输、可信验证。
* 安全区域边界：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：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、数据备份恢复、剩余信息保护、个人信息保护。
* 安全管理中心：系统管理、审计管理、安全管理、集中管控。

**2) 管理层面的差距评估（三级）内容：**

* 安全管理制度：安全策略、管理制度、制定与发布、评审与修订。
* 安全管理机构：岗位设置、人员配备、授权和审批、沟通与合作、审核和检查。
* 安全管理人员：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理。
* 安全建设管理：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、服务供应商管理。
* 安全运维管理：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。

## 等保加固辅导服务

1. 投标人根据等级保护基本要求以及风险和差距分析结果，对服务范围内信息系统的关键资产编制安全整改实施方案，实施方案中应包括加固风险分析及风险规避说明。派遣专业工程师到现场根据安全整改实施方案实施边界防护安全策略优化辅导、服务器病毒检查与清理，提供主机安全加固建议、数据库安全加固建议以及应用安全加固建议。安全整改实施后，根据整改实施情况提交《等级保护安全加固报告》。
2. 对于需要增加投资，部署新的信息安全产品和技术的整改措施，双方根据整改方案另行协商和实施。

## 等保制度建设服务

1. 投标人协助客户建设安全管理制度，为测评对象建立起信息安全策略、方针、各项安全管理制度、安全操作规范以及各类操作记录文档体系。
2. 提供涵盖等级保护基本要求所涉及的安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理5大类安全管理要求的方针、制度、各类记录表格模板，达到等级保护测评要求。提交《等级保护安全管理制度》。

## 等保测评辅助服务

投标人协助用户准备测评材料，指导用户单位配合测评机构开展等级测评工作，组织测评整改，并保障顺利通过等保测评获得测评报告。在测评阶段通过等级保护综合管理系统提实现等级测评管理，展示本单位各定级对象测评情况，包括定级对象测评状态、测评报告及测评相关文档信息；批量下载测评所需材料、填写测评结果，支持自定义编辑测评所需的各类文档，辅助等级测评工作。

## 等保台账管理服务

投标人通过服务工具等级保护综合管理系统提供等保台账管理服务，服务过程中提供各个定级对象等保咨询服务涉及到的各个环节产生的资料归档，支持对单个定级对象的定级、备案、自评、测评、管理制度五大维度的单独归档文件管理，并支持全部下载、按时间搜索按定级对象搜索等功能，服务结束后提供台账管理光盘，后续服务中可直接导入等保综合管理系统实现服务的延续。