福建信安网络科技有限公司

信安技〔2021〕

**关于福建省渔业资源监测中心实验室信息管理系统二期工程整改建议告知书**

**福建省渔业资源监测中心：**

2021年10月15日，我公司依据《信息安全技术 网络安全等级保护基本要求》，从安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面对您单位的福建省渔业资源监测中心实验室信息管理系统二期工程进行了现场测评及数据分析，发现尚存在部分安全隐患，我公司现将已发现的问题列出，并附上整改建议，详情请见附件：

（注：针对被测系统在本次等级测评过程中发现的安全问题，给出的部分整改建议有可能对实际运行的系统造成影响，请在实施整改前，组织相关人员对整改风险进行论证，并建立测试环境。）

联系人：郭镭

联系电话：18959261356

福建信安网络科技有限公司

二○二一年十月二十五日

1. **安全区域边界**

**云租户安全扩展要求**

|  |  |
| --- | --- |
| **安全控制点** | 安全审计 |
| **检测项** | [重要]a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启； |
| **检测结果** | 无法对云服务商和云服务客户在远程管理时执行的特权命令进行审计。 |
| **关联资产** | 云租户安全扩展要求 |
| **风险等级** | 中 |
| **整改建议** | 建议部署审计系统对云服务商和云服务客户在远程管理时执行的特权命令进行审计。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **服务器会话审计** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [重要]b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。 |
| **检测结果** | 云服务方对云服务客户系统和数据的操作无法被云租户审计。 |
| **关联资产** | 云租户安全扩展要求 |
| **风险等级** | 中 |
| **整改建议** | 建议部署审计系统审计云服务商对云服务客户系统和数据的操作，并将相关审计记录提供给云服务客户。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **服务器审计日志** |
| **测评复核** | **（测评机构填写）** |

1. **安全计算环境**

**实验室信息管理系统**

|  |  |
| --- | --- |
| **安全控制点** | 身份鉴别 |
| **检测项** | [重要]a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| **检测结果** | 应用系统通过内网登录，采用用户名+口令方式进行登录，身份标识唯一，但未配置口令复杂度及口令定期更换策略。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | **高** |
| **整改建议** | 建议应用系统配置口令复杂度策略和有效期策略，要求口令最小长度8位，必须包含数字、大小写字母和特殊符号，口令设置有效期（不超过90天）。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **用户新建控制密码规则**    修改密码控制    密码过期 |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 身份鉴别 |
| **检测项** | [重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| **检测结果** | 应用系统通过内网登录，未配置登录失败处理策略及登录连接超时策略。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | **高** |
| **整改建议** | 建议应用系统配置登录失败处理策略及登录超时时间，登录失败超过设定值，锁定账户或多重认证等，登录时间超过设定值（不超过30分钟），自动结束会话。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 身份鉴别 |
| **检测项** | [关键]c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| **检测结果** | 应用系统通过内网登录，使用HTTP协议进行远程管理，已使用MD5消息摘要算法对用户鉴别信息进行加密，但算法不安全。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议采用安全加密传输、使用加密协议等措施，防止鉴别信息在传输过程中被窃听。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **MD5基础上再加上国产加密算法**    采用https加密方式进行信息传输 |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]b)应重命名或删除默认账户，修改默认账户的默认口令； |
| **检测结果** | 应用系统未重命名默认账户，但修改了默认口令为复杂口令。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议锁定或删除默认账户。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对admin用户进行删除**  **删除前**    删除后 |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| **检测结果** | 应用系统设置了系统管理员、设备管理员、质量管理员、计量管理员等账户，未设置安全管理员、审计管理员等账户，未实现管理用户的权限分离。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议建立安全员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **建立安全员及审计员**      配置对应的权限 |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| **检测结果** | 应用系统审计日志仅授权用户可进行访问，但审计记录仅本地保存，未定期备份至日志服务器，无法对审计记录进行保护。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | **高** |
| **整改建议** | 建议部署日志服务器对日志进行集中存放，并确保保存时间能够达到半年以上。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对日志进行备份按日期进行保存** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| **检测结果** | 未对可远程管理应用系统的终端地址范围进行限制。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议对管理终端的网络地址范围进行限制。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **限制远程IP地址范围** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| **检测结果** | 未定期进行漏洞扫描，也未进行过补丁升级，在本次漏洞扫描、渗透测试结果中，发现系统存在中风险漏洞，未及时修复。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议定期进行漏洞扫描，并在测试通过的前提下，及时修复风险漏洞。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对系统进行安全扫描，并修复风险内容** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据完整性 |
| **检测项** | [重要]应采用校验技术保证重要数据在传输过程中的完整性。 |
| **检测结果** | 应用系统通过内网登录，使用HTTP协议进行数据传输，未采用校验技术保证重要数据在传输过程中的完整性。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议采用校验码技术或密码技术保证重要数据在传输过程中的完整性。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **重要数据使用国密加密**  **lQLPDhrT4mZtpxnNAlrNBKqwJRxFkPsw-skBiGTnBsAfAA_1194_602**  **采用https方式加密进行访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 系统所有数据仅在本地保存，未进行过备份。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | **高** |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **数据库做定时备份** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [重要]b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| **检测结果** | 系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议利用通信网络将重要数据定时批量传送至备用场地。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **定时备份数据库到备份服务器** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 个人信息保护 |
| **检测项** | [关键]a)应仅采集和保存业务必需的用户个人信息； |
| **检测结果** | 系统采集的用户个人信息包括姓名、科室、职位、联系电话、电子邮件等，均为业务必需的个人信息，未发现超范围采集情况，但未见个人信息保护的相关管理要求和流程。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议制定个人信息保护的相关管理要求和流程，确保个人信息能够得到合理保护，防止非法买卖、滥用。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **个人使用规则** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 个人信息保护 |
| **检测项** | [关键]b)应禁止未授权访问和非法使用用户个人信息。 |
| **检测结果** | 系统中保存的个人信息加密存储，仅授权用户可访问，非授权用户无法访问及使用，但未见个人信息保护的相关管理要求和流程。 |
| **关联资产** | 实验室信息管理系统 |
| **风险等级** | 中 |
| **整改建议** | 建议加强访问控制策略，对用户个人信息进行加密存储，禁止未授权访问和非法使用用户个人信息，并制定个人信息保护的相关管理要求和流程。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **个人信息管理** |
| **测评复核** | **（测评机构填写）** |

**云租户安全扩展要求**

|  |  |
| --- | --- |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)云服务客户应在本地保存其业务数据的备份； |
| **检测结果** | 云服务客户未在本地保存其业务数据的备份。 |
| **关联资产** | 云租户安全扩展要求 |
| **风险等级** | 中 |
| **整改建议** | 建议云服务客户在本地保存其业务数据的备份。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **系统管理员规则** |
| **测评复核** | **（测评机构填写）** |

**业务数据**

|  |  |
| --- | --- |
| **安全控制点** | 数据完整性 |
| **检测项** | [重要]应采用校验技术保证重要数据在传输过程中的完整性。 |
| **检测结果** | 应用系统通过内网登录，使用HTTP协议进行数据传输，未采用校验技术保证重要数据在传输过程中的完整性。 |
| **关联资产** | 业务数据 |
| **风险等级** | 中 |
| **整改建议** | 建议采用校验码技术或密码技术保证重要数据在传输过程中的完整性。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **使用国产加密**  **lQLPDhrT4mZtpxnNAlrNBKqwJRxFkPsw-skBiGTnBsAfAA_1194_602**  **通过https证书进行访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 系统所有数据仅在本地保存，未进行过备份。 |
| **关联资产** | 业务数据 |
| **风险等级** | **高** |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **定时备份数据库** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [重要]b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| **检测结果** | 系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 |
| **关联资产** | 业务数据 |
| **风险等级** | 中 |
| **整改建议** | 建议利用通信网络将重要数据定时批量传送至备用场地。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **管理制度数据组需要进行备份** |
| **测评复核** | **（测评机构填写）** |

**个人信息**

|  |  |
| --- | --- |
| **安全控制点** | 数据完整性 |
| **检测项** | [重要]应采用校验技术保证重要数据在传输过程中的完整性。 |
| **检测结果** | 应用系统通过内网登录，使用HTTP协议进行数据传输，未采用校验技术保证重要数据在传输过程中的完整性。 |
| **关联资产** | 个人信息 |
| **风险等级** | 中 |
| **整改建议** | 建议采用校验码技术或密码技术保证重要数据在传输过程中的完整性。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **系统中无重要个人信息，如身份证手机号等；**  **对用户信息进行加密处理**      https证书进行访问 |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 系统所有数据仅在本地保存，未进行过备份。 |
| **关联资产** | 个人信息 |
| **风险等级** | **高** |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **定时备份** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [重要]b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| **检测结果** | 系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 |
| **关联资产** | 个人信息 |
| **风险等级** | 中 |
| **整改建议** | 建议利用通信网络将重要数据定时批量传送至备用场地。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **技术科通过网络进行服务器备份** |
| **测评复核** | **（测评机构填写）** |

**应用服务器**

|  |  |
| --- | --- |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]a)应对登录的用户分配账户和权限； |
| **检测结果** | 未对可登录的用户分配账户和权限，仅有administrator账户。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议对可登录的用户分配账户和权限。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **单独用户管理** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]b)应重命名或删除默认账户，修改默认账户的默认口令； |
| **检测结果** | 为重命名默认账户administrator，但已设置了复杂口令。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议锁定或删除默认账户。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **已经对administrator进行处理** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| **检测结果** | 服务器中未发现多余或过期的账户，但所有运维人员均通过同一账户登录，存在共享账户的情况。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议为每个管理员分别创建不同账户，保证不同管理员使用不同账户进行管理。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **不同角色通过不通用户进行登录** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| **检测结果** | 服务器仅设置了系统管理员账户，未设置安全管理员、审计管理员等账户，未实现管理用户的权限分离。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议建立安全员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **建立审计员，安全员账户** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| **检测结果** | 服务器未开启安全审计功能，无法对重要的用户行为和重要安全事件进行审计。 |
| **关联资产** | 应用服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，对重要的用户行为和重要安全事件进行审计。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **开启审计，包含成功和失败** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]b)审计记录应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； |
| **检测结果** | 服务器未开启安全审计功能，无相关审计记录。 |
| **关联资产** | 应用服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，审计日志至少包含事件的日期和时间、用户、事件类型、事件是否成功等相关信息。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **同步时间保证时间准确性** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| **检测结果** | 服务器未开启安全审计功能，无其它审计记录保护措施，无相关审计记录。 |
| **关联资产** | 应用服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，并对审计记录进行保护，避免受到未预期的删除、修改或覆盖。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **只允许管理员进行操作** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [关键]b)应关闭不需要的系统服务、默认共享和高危端口； |
| **检测结果** | 服务器存在不必要的默认共享，未关闭135、445等不必要的端口。 |
| **关联资产** | 应用服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议关闭不必要的服务，关闭不必要的端口，仅开启业务所需的服务及端口。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **禁止对应端口进行访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| **检测结果** | 未对可远程管理服务器的终端地址范围进行限制。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议对管理终端的网络地址范围进行限制。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **针对可以远程到服务器的进行地址范围限制** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| **检测结果** | 未进行过漏洞扫描，无法及时发现系统漏洞。 |
| **关联资产** | 应用服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议定期进行漏洞扫描，并在测试通过的前提下，及时修复高风险漏洞。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **进行扫描，进行处理存在的风险漏洞** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 可信验证 |
| **检测项** | [一般]可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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| **检测结果** | 未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。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 低 |
| **整改建议** | 建议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，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 服务器每天在云平台进行快照备份，但未使用备份文件进行过恢复测试。 |
| **关联资产** | 应用服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **创建服务器定时备份** |
| **测评复核** | **（测评机构填写）** |

**数据库服务器**

|  |  |
| --- | --- |
| **安全控制点** | 身份鉴别 |
| **检测项** | [重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| **检测结果** | 服务器已配置非法登录10次后锁定账户30分钟，但未配置登录连接超时自动退出策略。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议配置登录连接超时策略，严格限制登录超时时间。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **已配置** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]a)应对登录的用户分配账户和权限； |
| **检测结果** | 未对可登录的用户分配账户和权限，仅有administrator账户。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议对可登录的用户分配账户和权限。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **新增分配可登录账户** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]b)应重命名或删除默认账户，修改默认账户的默认口令； |
| **检测结果** | 为重命名默认账户administrator，但已设置了复杂口令。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议锁定或删除默认账户。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **已修改默认账户administrator** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| **检测结果** | 服务器中未发现多余或过期的账户，但所有运维人员均通过同一账户登录，存在共享账户的情况。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议为每个管理员分别创建不同账户，保证不同管理员使用不同账户进行管理。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **创建不同账户进行使用** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| **检测结果** | 服务器仅设置了系统管理员账户，未设置安全管理员、审计管理员等账户，未实现管理用户的权限分离。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议建立安全员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **创建安全员账户，审计员账户** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| **检测结果** | 服务器未开启安全审计功能，无法对重要的用户行为和重要安全事件进行审计。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，对重要的用户行为和重要安全事件进行审计。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **开启审核策略** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]b)审计记录应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； |
| **检测结果** | 服务器未开启安全审计功能，无相关审计记录。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，审计日志至少包含事件的日期和时间、用户、事件类型、事件是否成功等相关信息。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **同步网络时间保证准确性，日志已保护日期和类型等** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| **检测结果** | 服务器未开启安全审计功能，无其它审计记录保护措施，无相关审计记录。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议开启审计日志功能，并对审计记录进行保护，避免受到未预期的删除、修改或覆盖。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **只允许管理员才能对系统进行操作** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [关键]b)应关闭不需要的系统服务、默认共享和高危端口； |
| **检测结果** | 服务器存在不必要的默认共享，未关闭135、445等不必要的端口。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议关闭不必要的服务，关闭不必要的端口，仅开启业务所需的服务及端口。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **已经禁止了135和445端口访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| **检测结果** | 未对可远程管理服务器的终端地址范围进行限制。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议对管理终端的网络地址范围进行限制。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **限制特定的ip进行访问远程** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| **检测结果** | 未进行过漏洞扫描，无法及时发现系统漏洞。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | **高** |
| **整改建议** | 建议定期进行漏洞扫描，并在测试通过的前提下，及时修复高风险漏洞。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **扫描并且处理存在的漏洞** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 可信验证 |
| **检测项** | [一般]可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，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| **检测结果** | 未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。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 低 |
| **整改建议** | 建议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，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 服务器每天在云平台进行快照备份，但未使用备份文件进行过恢复测试。 |
| **关联资产** | 数据库服务器 |
| **风险等级** | 中 |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **建立数据库服务器定时备份机制** |
| **测评复核** | **（测评机构填写）** |

**IIS中间件**

|  |  |
| --- | --- |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| **检测结果** | 未定期进行漏洞扫描，也未进行过补丁升级。 |
| **关联资产** | IIS中间件 |
| **风险等级** | 中 |
| **整改建议** | 建议定期进行漏洞扫描，并在测试通过的前提下，及时修复风险漏洞。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对IIS数据中间件进行扫描** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | IIS中间件配置文件在本地服务器中保存，服务器通过快照的方式每天增量备份，每周全量备份，但未使用备份文件进行过备份恢复测试。 |
| **关联资产** | IIS中间件 |
| **风险等级** | 中 |
| **整改建议** | 建议建立备份恢复机制，定期对备份的数据进行恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对IIS进行备份并定期备份** |
| **测评复核** | **（测评机构填写）** |

**SqlServer数据库**

|  |  |
| --- | --- |
| **安全控制点** | 身份鉴别 |
| **检测项** | [重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| **检测结果** | 数据库未配置登录失败锁定策略及登录连接超时自动退出策略。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议数据库配置登录失败处理策略，防止恶意人员暴力破解账户口令。并配置登录连接超时策略，降低设备被非授权访问的风险。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **通过账户登录失败处理进行账户锁定** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]a)应对登录的用户分配账户和权限； |
| **检测结果** | 数据库仅使用超级管理员账户fjhy进行管理，该账户具有最大权限。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议严格限制系统管理账户的远程访问权限，禁止其进行远程登录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **配置指定客户端IP进行访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [重要]c)应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| **检测结果** | 数据库中未发现多余或过期的账户，但所有运维人员均通过同一账户登录，存在共享账户的情况。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议为每个管理员分别创建不同账户，保证不同管理员使用不同账户进行管理。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **创建不同的账户jczx进行管理** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 访问控制 |
| **检测项** | [一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| **检测结果** | 数据库仅设置了系统管理员账户fjhy，未设置安全管理员、审计管理员等账户，未实现管理用户的权限分离。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议建立安全员、审计员账户，并根据业务需要设置各账户的权限，实现管理权限最小化。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **创建安全员和审计员登录用户权限** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全审计 |
| **检测项** | [一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| **检测结果** | 数据库审计日志仅授权用户可进行访问，但审计记录仅本地保存，未定期备份至日志服务器，无法对审计记录进行保护。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | **高** |
| **整改建议** | 建议部署日志服务器对日志进行集中存放，并确保保存时间能够达到半年以上。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对数据库进行定时备份** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| **检测结果** | 未对可远程管理数据库的终端地址范围进行限制。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | **高** |
| **整改建议** | 建议对管理终端的网络地址范围进行限制。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **限制连接客户端的ip进行控制** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 入侵防范 |
| **检测项** | [重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| **检测结果** | 未定期进行漏洞扫描，也未进行过补丁升级。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | **高** |
| **整改建议** | 建议定期进行漏洞扫描，并在测试通过的前提下，及时修复风险漏洞。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对数据库进行安全扫描** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据完整性 |
| **检测项** | [重要]应采用校验技术保证重要数据在传输过程中的完整性。 |
| **检测结果** | 数据库未采用校验技术保证重要数据在传输过程中的完整性。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议采用校验码技术或密码技术保证重要数据在传输过程中的完整性。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **使用了云服务器，并使用了商密**  **1635850669(1)**  **使用https访问** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [关键]a)应提供重要数据的本地数据备份与恢复功能； |
| **检测结果** | 系统所有数据仅在本地保存，未进行过备份。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议建立备份恢复机制，定期对重要数据进行备份以及恢复测试，确保在出现数据破坏时，可利用备份数据进行恢复。并妥善保存相关记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **数据库定期备份** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 数据备份恢复 |
| **检测项** | [重要]b)应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| **检测结果** | 系统备份数据仅在本地保存，未利用通信网络将关键数据定时批量传送至备用场地。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议利用通信网络将重要数据定时批量传送至备用场地。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **定期对数据库备份到服务器** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 个人信息保护 |
| **检测项** | [关键]a)应仅采集和保存业务必需的用户个人信息； |
| **检测结果** | 系统采集的用户个人信息包括姓名、科室、职位、联系电话、电子邮件等，均为业务必需的个人信息，未发现超范围采集情况，但未见个人信息保护的相关管理要求和流程。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议制定个人信息保护的相关管理要求和流程，确保个人信息能够得到合理保护，防止非法买卖、滥用。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **严格现在访问权限和控制保密等** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 个人信息保护 |
| **检测项** | [关键]b)应禁止未授权访问和非法使用用户个人信息。 |
| **检测结果** | 系统中保存的个人信息加密存储，仅授权用户可访问，非授权用户无法访问及使用，但未见个人信息保护的相关管理要求和流程。 |
| **关联资产** | SqlServer数据库 |
| **风险等级** | 中 |
| **整改建议** | 建议加强访问控制策略，对用户个人信息进行加密存储，禁止未授权访问和非法使用用户个人信息，并制定个人信息保护的相关管理要求和流程。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **严格现在访问权限和控制保密等**    系统使用权限 |
| **测评复核** | **（测评机构填写）** |

1. **安全管理制度**

|  |  |
| --- | --- |
| **安全控制点** | 制定和发布 |
| **检测项** | [一般]a)应指定或授权专门的部门或人员负责安全管理制度的制定； |
| **检测结果** | 未指定或授权专门的部门或人员负责安全管理制度的制定工作。 |
| **关联资产** | 安全管理制度 |
| **风险等级** | 低 |
| **整改建议** | 建议公司指定并在制度文档中明确专门负责信息安全制度制定相关工作的人员或部门。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 评审和修订 |
| **检测项** | [重要]应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。 |
| **检测结果** | 未对安全管理制度的合理性和适用性进行过论证和审定。 |
| **关联资产** | 安全管理制度 |
| **风险等级** | 中 |
| **整改建议** | 建议在制度中明确对安全管理制度需进行定期或不定期的论证和审定工作，并在实际工作中遵照相关制度执行。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **安全管理员定期提出安全意见**    系统使用 |
| **测评复核** | **（测评机构填写）** |

1. **安全管理机构**

|  |  |
| --- | --- |
| **安全控制点** | 授权和审批 |
| **检测项** | [一般]a)应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； |
| **检测结果** | 未根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等内容。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 低 |
| **整改建议** | 建议制定《部门职责文档》、《岗位职责文档》，明确各部门和岗位的授权审批事项。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 授权和审批 |
| **检测项** | [重要]b)应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程。 |
| **检测结果** | 未对系统变更、重要操作、物理访问和系统接入等事项进行审批。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 中 |
| **整改建议** | 建议针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **变更审批表** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 沟通和合作 |
| **检测项** | [重要]a)应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； |
| **检测结果** | 未定期与各类管理人员、组织内部机构和网络安全管理部门之间进行合作沟通，不具备沟通合作记录。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 中 |
| **整改建议** | 建议加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 沟通和合作 |
| **检测项** | [一般]b)应加强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； |
| **检测结果** | 未定期与网络安全职能部门、各类供应商、业界专家及安全组织等进行合作沟通，不具备沟通合作记录。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 低 |
| **整改建议** | 建议加强与公安机关、供应商、业界专家、专业的安全公司、安全组织的合作与沟通。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 沟通和合作 |
| **检测项** | [一般]c)应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
| **检测结果** | 未建立外联单位联系列表。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 低 |
| **整改建议** | 建议建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 审核和检查 |
| **检测项** | [一般]应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |
| **检测结果** | 未定期进行常规安全检查。 |
| **关联资产** | 安全管理机构 |
| **风险等级** | 低 |
| **整改建议** | 建议安全管理员定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |

1. **安全管理人员**

|  |  |
| --- | --- |
| **安全控制点** | 安全意识教育和培训 |
| **检测项** | [重要]应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 |
| **检测结果** | 未对各个岗位人员进行安全教育和岗位技能培训，并告知相关的安全责任和惩戒措施。 |
| **关联资产** | 安全管理人员 |
| **风险等级** | 中 |
| **整改建议** | 建议对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，并告知相关的安全责任和惩戒措施。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **安全教育培训制度**  **1635319420(1)** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 外部人员访问管理 |
| **检测项** | [重要]a)应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； |
| **检测结果** | 未对外部人员访问受控区域做出规定，也未由专人全程进行陪同。 |
| **关联资产** | 安全管理人员 |
| **风险等级** | 中 |
| **整改建议** | 建议外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **第三方人员管理制度** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 外部人员访问管理 |
| **检测项** | [重要]b)应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； |
| **检测结果** | 外部人员接入受控网络无需提交书面申请。 |
| **关联资产** | 安全管理人员 |
| **风险等级** | 中 |
| **整改建议** | 建议外部人员受控网络前先提出书面申请，批准后由由专人开设账户、分配权限，并登记备案。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **第三方人员申请及授权** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 外部人员访问管理 |
| **检测项** | [重要]c)外部人员离场后应及时清除其所有的访问权限。 |
| **检测结果** | 外部人员在离开受控区域及断开受控网络后，未及时清除其访问权限，不具备相关记录。 |
| **关联资产** | 安全管理人员 |
| **风险等级** | 中 |
| **整改建议** | 建议在外部人员离场后应及时清除其所有的访问权限，并保留清除记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **第三方人员管理** |
| **测评复核** | **（测评机构填写）** |

1. **安全建设管理**

|  |  |
| --- | --- |
| **安全控制点** | 安全方案设计 |
| **检测项** | [重要]c)应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。 |
| **检测结果** | 系统安全设计方案的论证和审定管理不完善，缺少对系统安全策略相关配套文件的合理性和正确性的论证和审定记录。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 中 |
| **整改建议** | 建议组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **安全方案，安全审计报告等** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 外包软件开发 |
| **检测项** | [重要]a)应在软件交付前检测其中可能存在的恶意代码； |
| **检测结果** | 未在软件交付前通过第三方检测工具或人工检测软件包中可能存在的恶意代码。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 中 |
| **整改建议** | 建议在交付前对开发单位提供软件源代码中可能存在的恶意代码通过第三方的检查工具或人工进行审查，并保留相关检查报告。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **通过恶意代码检查扫描分析** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 工程实施 |
| **检测项** | [一般]a)应指定或授权专门的部门或人员负责工程实施过程的管理； |
| **检测结果** | 未指定或授权专门的部门或人员负责工程实施过程的管理。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 低 |
| **整改建议** | 建议指定或授权专门的部门或人员负责工程实施过程的管理。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 工程实施 |
| **检测项** | [一般]b)应制定安全工程实施方案控制工程实施过程。 |
| **检测结果** | 未提供详细的工程实施方案，来明确项目实施过程、方法、项目进度及项目质量管理等内容。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 低 |
| **整改建议** | 建议补充提供工程实施方案，对项目实施过程、方法、项目进度及项目质量管理等内容进行明确，并根据实际情况对实施过程进行记录，达到控制的目的。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 测试验收 |
| **检测项** | [一般]a)应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； |
| **检测结果** | 系统交付之前未经过标准的验收过程，未编制过验收方案，未依据方案出具验收报告。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 低 |
| **整改建议** | 建议制定详细的测试验收方案，并对测试结果进行详细的记录，形成测试验收报告。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **对系统进行整理测试** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 测试验收 |
| **检测项** | [关键]b)应进行上线前的安全性测试，并出具安全测试报告。 |
| **检测结果** | 系统上线前未对系统进行安全性测试验收。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 中 |
| **整改建议** | 建议系统上线前测试中加入安全性测试内容，并遵照国家密码管理局印发的有关规定执行密码应用安全性测试或测评工作。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **安全测试报告** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 系统交付 |
| **检测项** | [一般]b)应对负责运行维护的技术人员进行相应的技能培训； |
| **检测结果** | 系统运维人员未接受过任何形式的技能培训。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 中 |
| **整改建议** | 建议定期对系统运维人员进行技能培训，并保存培训记录，以保证系统平稳运行。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **培训记录文档** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 等级测评 |
| **检测项** | [重要]b)应在发生重大变更或级别发生变化时进行等级测评； |
| **检测结果** | 在确定该信息系统的安全保护等级后，并未发生较大变更，未调整安全保护级别，但未规定系统发生重大变更或级别发生变化时及时进行等级测评。 |
| **关联资产** | 安全建设管理 |
| **风险等级** | 中 |
| **整改建议** | 建议相关单位在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **制度管理评测及改造制度** |
| **测评复核** | **（测评机构填写）** |

1. **安全运维管理**

|  |  |
| --- | --- |
| **安全控制点** | 资产管理 |
| **检测项** | [一般]应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 |
| **检测结果** | 未编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议编制并保存与信息系统相关的资产清单，包括但不限于资产责任部门、重要程度和所处位置等内容。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 介质管理 |
| **检测项** | [一般]a)应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； |
| **检测结果** | 未建立对介质的存放环境、使用、维护和销毁等方面作出规定的介质安全管理制度。 |
| **关联资产** | 安全运维管理 |
| **风险等级** |  |
| **整改建议** | 建议建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 介质管理 |
| **检测项** | [一般]b)应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。 |
| **检测结果** | 未对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，未对介质归档和查询等进行登记记录。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 设备维护管理 |
| **检测项** | [一般]a)应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； |
| **检测结果** | 未对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 设备维护管理 |
| **检测项** | [一般]b)应对配套设施、软硬件维护管理做出规定，包括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。 |
| **检测结果** | 未建立指导运维人员对设备进行维护操作的设备操作维护手册。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议建立并完善系统设备操作维护手册，系统运行维护人员严格按照系统操作维护手册进行操作，规范系统操作管理。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 漏洞和风险管理 |
| **检测项** | [重要]应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。 |
| **检测结果** | 未对系统进行漏洞扫描及渗透测试。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 中 |
| **整改建议** | 建议指定专人定期对网络和主机进行恶意代码检测并保存检测记录。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **服务器通过省政务云服务器管理，管理方做对应处理。** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 网络和系统安全管理 |
| **检测项** | [一般]b)应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； |
| **检测结果** | 未指定专门的部门或人员进行账户管理。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。 |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 网络和系统安全管理 |
| **检测项** | [一般]d)应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； |
| **检测结果** | 未建立重要设备的配置和操作手册，并按照操作手册进行进行安全配置和优化配置。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 中 |
| **整改建议** | 建议保留重要设备或系统（操作系统、数据库、网络设备）配置和操作手册，可依据手册对设备进行安全配置和优化配置。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **设备操作手册** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 网络和系统安全管理 |
| **检测项** | [一般]e)应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。 |
| **检测结果** | 不具备详细的运维操作日志，日志内容仅包括时间及人员等。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 低 |
| **整改建议** | 建议详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； |
| **整改情况** | **（需要文字描述和贴图证明）** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 变更管理 |
| **检测项** | [重要]应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。 |
| **检测结果** | 未制定变更相关制度，明确变更前需根据变更需求制定变更方案，且未规定变更方案的申报审批程序。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 中 |
| **整改建议** | 建议制定系统变更相关制度，规定变更方案的申报审批程序，应要求方案包含变更类型、变更原因、变更过程、变更前评估等内容。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **变更管理办法** |
| **测评复核** | **（测评机构填写）** |
|  |  |
| **安全控制点** | 安全事件处置 |
| **检测项** | [重要]c)应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。 |
| **检测结果** | 在安全事件报告和响应处理过程中，未分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训等。 |
| **关联资产** | 安全运维管理 |
| **风险等级** | 中 |
| **整改建议** | 建议在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。 |
| **整改情况** | **（需要文字描述和贴图证明）**  **安全事件管理办法** |
| **测评复核** | **（测评机构填写）** |