风险检查项明细清单

序号	5A安全架构	分类	风险检查项	检查内容	参考检查点	对象	范围
3	身份认证 Authentication	口令密码	弱口令风险	是否符合弱口令检查要求，如包含大小写字母、数字、特殊符号等8位以上，对弱密码进行定期提醒。	1、用户输入密码场景使用强密码验证 2、检查规则为大小写字母+数字+特殊符号 3、服务端验证密码长度要求至少8位 4、对系统已存在的弱密码定期提醒修改推送	应用系统	登录输入密码界面
4			口令存储未加密风险	口令信息是否进行加密存储，如使用增加盐值、Hash等不可逆加密算法，提升口令存储安全。	1、用户密码信息使用加密存储 2、加密方式使用不可逆的算法	数据存储介质	口令存储表字段
5			Ticket验证缺失风险	登录是否为服务端认证方式，返回Ticket作为用户临时身份。	1、输入正确的用户名密码后，服务端返回唯一标识（Ticket）作为用户临时身份	应用系统	登录认证API接口
6			AppKey认证缺失风险	服务器端接口调用采用AppKey换取动态Token方式，保证Token有效期不超过6小时。	1、服务端接口调用使用AppKey认证方式 2、Token有效期不超过6小时	应用系统	服务端接口
7			密码未加密传输风险	密码传输使用了https，且采用密文加密传输。	1、密码传输链路采用HTTPS协议 2、密码进行前端加密后，从前端传输到服务器端	应用系统	登录认证
8			账号密码找回风险	具备账号密码找回逻辑缺陷防护能力。	1、系统是否具备用户账号密码找回功能 2、账号密码找回进行用户身份识别（手机短信/人脸识别）	应用系统	找回密码页面
9			认证接口存在敏感信息风险	认证接口不存在敏感信息返回，避免敏感信息泄露。	1、认证接口只返回用户认证通过的临时身份标识 2、用户临时身份标识为无规律不可预测的字符串	应用系统	认证接口
10			账号信息未加密风险	建立账号泄露防护机制，比如手机号、身份证号等关键信息加密。	1、对手机号、身份证进行加密存储	应用系统	账号存储
14	授权 Authorization	权限分配	水平越权风险	未经授权，用户A不能访问用户B的信息资源。	1、服务器端对用户访问数据进行权限验证	应用系统	权限验证
15			垂直越权越权风险	未经授权，低权限用户不可获得高权限。	1、高权限操作服务器端进行用户权限验证	应用系统	权限验证
31			开发测试风险	各应用模块是否执行了开发安全检查规范，确保开发环境、代码仓库安全，未使用站外的JS、图片、音视频、链接或文本，系统经过了黑白盒安全测试，并出具安全测试报告。	1、有安全开发规范制度 2、应用系统定期进行渗透测试 3、应用系统定期进行代码审计	应用系统	开发规范 安全测试

序号	5A安全架构	分类	风险检查项	检查内容	参考检查点	对象	范围
32	资产保护 Asset Protection	应用层	运行维护风险	系统发布、变更是否经过安全基线、代码加固、App加固等安全措施，稳定运行过程中具备安全风险监测能力，并进行周期安全巡检。	1、系统发布/变更经过安全基线检查 2、系统发布/变更经过代码加固审核 3、系统发布/变更经过APP（如涉及）加固审核 4、系统运行时有安全攻击监测能力 5、系统运行时进行每天一次安全巡检	应用系统	应用运维
35		数据层	数据存储风险	系统数据存储在政务云环境，并定期进行远程备份，关键敏感数据进行加密存储。	1、执行定期的数据备份和恢复 2、对关键敏感数据进行加密存储	应用系统	数据存储
41		基础资源层	网络风险	应用所使用的网络是否具备网络入侵防护能力，各专有网络边界是否部署防火墙、网闸、流量监测等安全防护设备。	1、应用系统所在网络边界部署安全防护设备	应用系统	网络层