软件安全开发服务资质认证自评估表

组织名称		**申报级别**	
评估时间		**评估部门/人员**	

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
1.	服务技术要求	建立软件安全开发服务流程。	软件安全开发服务流程，流程图中应包括每个阶段对应的职责、输入输出等。			
2.		制定软件安全开发服务规范并按照规范实施。	软件安全开发服务规范并按照规范实施。			
3.	准备阶段	建立软件项目安全开发团队，明确各岗位、人员、职责。	项目人员构成表或其他能体现项目组成员构成的文档，其中明确项目组成员构成情况以及安全开发人员的角色及职责。			
4.		制定软件项目安全开发管理计划，明确开发过程管控措施。	项目开发计划，计划中应包含安全开发的内容。			
5.		建立软件开发的配置管理计划，明确配置管理的安全要求。	项目配置管理计划，包含安全相关活动。提供配置管理相关记录。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
6.		建立变更控制制度，明确软件项目变更控制的安全要求。	变更控制管理制度，提供项目变更控制记录，变更的记录单，记录单中的内容应包含变更申请，审批，执行，执行后的评价结果。			
7.		制定软件项目安全培训计划，对相关人员进行安全培训。	培训管理制度，项目培训计划和培训记录。			
8.		建立独立的开发环境，确保开发环境与运行环境隔离。	开发环境与运行环境配置的说明文档。			
9.		**仅二级/一级要求：**建立软件安全开发项目风险管理机制，对软件项目进行风险评估。	风险管理制度、风险管理计划、风险分析报告。			
10.		**仅二级/一级要求：**使用配置管理工具对软件项目进行配置管理。	配置管理计划，其中描述采用的配置管理工具；配置管理工具的使用情况介绍。			
11.		**仅二级/一级要求：**配备专职的测试人员。	项目人员构成表或其他能体现项目组成员构成的文档，设立专职的测试人员，并明确描述其职责。			
12.		**仅二级/一级要求：**建立独立的测试环境，确保测试环境与开发环境隔离。	开发环境与测试环境配置的说明文档。			
13.		**仅一级要求：**建立软硬件设备和工具等资源安全使用规范。	软硬件设备及工具安全使用规范；软硬件设备及工具资源配备计划。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
14.		**仅一级要求：**配备安全管理人员。	安全管理专职人员的任命文件，项目相关的安全监控记录。			
15.		**仅一级要求：**建立变更控制委员会。	变更控制委员会成员构成与职责规定文件。			
16.	需求阶段	调研项目背景信息，收集项目需求，明确软件功能、性能及安全方面的要求。	需求阶段控制程序文件；需求阶段项目文档，包括可行性报告、招标文件、需求分析报告等，需求文档的内容应涉及软件功能、性能及安全性要求。			
17.		结合软件项目需求、安全需求，与客户充分沟通，达成共识并形成记录。	与客户沟通的记录。			
18.		**仅二级/一级要求：**准确识别和综合分析软件项目在可用性、完整性、真实性、机密性、不可否认性、可控性和可靠性等方面的安全需求。	需求分析报告，内容应覆盖条款的要求。			
19.		**仅二级/一级要求：**对于数据采集、产生、使用，明确识别安全保护要求。				
20.		**仅二级/一级要求：**基于客户需求，开展需求分析，编制具有软件安全需求的分析报告。				
21.		**仅二级/一级要求：**需求分析报告中明确项目开发中使用的安全技术标准、规范。				

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
22.		**仅一级要求：**应基于软件安全威胁开展需求分析。				
23.		**仅一级要求：**基于软件项目需求分析建立软件安全开发模型。				
24.	设计阶段	根据软件项目需求，编制软件设计说明书。	设计阶段控制程序文件；提供软件设计说明书，内容应覆盖条款的要求。			
25.		软件设计说明书明确系统/子系统的功能和非功能设计要求。				
26.		软件设计说明书明确包含安全功能要求，包括标识与鉴别、访问控制、安全审计和安全管理等。				
27.	设计阶段-概要设计	**仅二级/一级要求：**概要设计说明书应明确数据完整性和保密性、通信完整性和保密性、软件容错、资源控制等安全功能要求。	设计阶段控制程序文件；提供概要设计说明书，内容应覆盖条款的要求。			
28.		**仅一级要求：**概要设计说明书中应明确基于软件安全威胁分析的安全要求。				
29.		**仅一级要求：**当开发场景适用时，概要设计说明书中应明确抗抵赖、安全标记、可信路径等安全功能要求。				

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
30.	设计阶段-详细设计	**仅二级/一级要求：**详细设计说明书中应包含对数据产生、传输、存储、使用、处理和归档安全方面的详细设计。	详细设计说明书，内容应覆盖条款的要求。			
31.		**仅一级要求：**依据安全要求和概要设计说明书，明确基于软件安全威胁分析进行详细设计。				
32.	编码阶段	制定统一的代码安全编码规范，确保开发人员参照规范安全编码。	软件开发所使用语言的安全编码规范，规范内容包括但不限于代码安全编写的原则、方式、方法等。			
33.		依据详细设计说明书，对软件进行安全编码。	在编码过程中，对规避高危风险的漏洞采取的方法或措施的文档或记录。			
34.		软件代码要经过安全检查、评审，对于发现的漏洞能有效修复。	代码安全检查、评审记录，对发现的漏洞，提供漏洞修复与验证记录。			
35.		**仅二级/一级要求：**软件代码的安全检查、评审工作应形成记录。	代码检查、审核相关记录。			
36.		**仅一级要求：**采用自动化工具对代码安全漏洞进行审查，对于发现的漏洞能有效修复，并形成审查报告。	代码检查工具的检查结果记录/报告。			
37.	测试阶段	依据软件设计说明书对软件功能、安全功能进行测试。	测试方案、测试计划，提供软件功能测试、安全性测试记录与报告。			
38.		对测试发现的漏洞进行分析并有效修	漏洞发现、分析与修复的记录。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		复。				
39.	测试阶段-单元测试	**仅二级/一级要求：**明确单元测试策略，制定单元测试计划。	单元测试的测试策略、测试计划。			
40.		**仅二级/一级要求：**依据详细设计说明书和测试计划进行单元测试设计，并执行单元测试，形成测试记录。	单元测试用例设计、测试记录。			
41.		**仅一级要求：**对单元测试结果进行分析，形成分析报告。	单元测试分析报告。			
42.	测试阶段-集成测试	**仅二级/一级要求：**明确集成测试策略，制定集成测试计划。	集成测试的测试策略、测试计划。			
43.		**仅二级/一级要求：**依据概要设计方案和测试计划进行集成测试设计，并执行集成测试，形成测试记录。	集成测试用例设计、测试记录。			
44.		**仅一级要求：**对集成测试结果进行分析，形成分析报告。	集成测试分析报告。			
45.	测试阶段-系统测试	**仅二级/一级要求：**制定包括系统安全性测试在内的测试计划，并执行系统测试，形成测试记录。	安全性测试计划和测试用例设计文档、测试记录。			
46.						
47.						

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		仅二级/一级要求：基于软件安全功能的安全要求，制定脆弱性测试方案，对安全漏洞进行测试，形成测试记录。	脆弱性测试方案、测试记录。			
48.		**仅二级/一级要求：**对系统测试结果进行分析，形成分析报告。	测试分析报告，其中包括软件安全测试的结果分析。			
49.		**仅一级要求：**基于软件项目的安全要求，制定系统渗透性测试方案，模拟攻击场景，对系统安全性进行测试，并形成分析报告。	渗透性测试方案、渗透测试记录和渗透测试报告。			
50.	验收阶段-系统试运行	测试系统运行的可靠性、稳定性和安全性，进行试运行，并记录系统运行状况，试运行周期至少一个月。	系统试运行相关记录。			
51.		基于系统试运行相关记录，及时对软件进行调整、维护。	系统调整、维护记录。			
52.		**仅二级/一级要求：**试运行结束后，制定系统试运行报告，并提交客户。	系统试运行报告。			
53.		**仅一级要求：**提供三个月以上的试运行记录和报告。	系统试运行记录和报告。			
54.		**仅一级要求：**综合软件系统试运行状态，	系统运行策略、安全指南。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		建立软件系统运行策略和安全指南。				
55.	验收阶段-验收交付	根据合同约定，向客户提交完整的项目资料及交付物，并提出验收申请。	验收申请、验收资料、验收报告。			
56.		根据合同约定，进行项目验收，形成项目验收报告。				
57.		**仅二级/一级要求：**提交软件安全测评报告。	软件安全测评报告。			
58.		**仅一级要求：**提交软件产品第三方安全专家/第三方权威机构出具的软件产品安全测评报告或安全认证证书。	软件产品第三方安全专家/第三方权威机构出具的软件产品安全测评报告或安全认证证书。			
59.	维保阶段	对于影响软件系统安全、稳定运行的缺陷，及时有效采取打补丁、版本升级等方式予以消除，并提供远程技术支持服务。	巡查记录、故障记录、升级记录等。			
60.		**仅二级/一级要求：**制定系统运行计划、安全事件响应计划、安全事件应急预案，建立应急响应服务保障团队。	系统运行计划、安全事件响应计划、安全事件应急预案；应急保障团队人员组织构成和职责规定文件；应急事件记录。			
61.		**仅二级/一级要求：**及时应对突发安全事件，并向用户提供安全事件解决报告。				
62.		**仅一级要求：**制定软件健康检查计划、方案，定期实施，提交相应的系统健康检查报告、巡检报告。	健康检查计划、方案、系统健康检查报告、巡检报告、系统优化改进记录。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
63.		**仅一级要求：**根据健康检查报告进行分析，持续优化系统。				
64.	**上一年度提出的观察项整改情况（如有）**					
65.						
66.						
67.	**上一年度提出的不符合项整改情况（如有）**					
68.						
69.						

自评估结论：

经自主评估，本单位的软件安全开发服务满足《信息安全服务 规范》____级要求，申请第三方审核。

本单位郑重承诺，《信息安全服务资质认证自评估表-公共管理》与本自评估表中所提供全部信息真实可信，且均可提供相应证明材料。

智汇源认证


罗 龙 总 监
重庆智汇源认证服务有限公司
139 8308 6348 023-6778 8950
重庆市江北区北滨二路538号7-8-4
www.cqzhihuiyuan.com
成都智汇源认证服务有限公司
136 0808 9100 028-8430 1286
成都市高新区天府三街218号1-10-8
www.sczhihuiyuan.com


认证范围：军工武器产品认证；海陆空产品认证；信息安全资质认证；
特种行业资质认证；实验室资质认证；管理体系标准认证；
CNAS
CMA
计量授权
CCC f
API
武器装备军标认证
武器装备保密资格
武器装备科研许可
武器装备承制注册
涉密信息系统集成
航空航天AS9100
CRCC
CCS
IATF 16949
CCRC 信息安全资质
LA
特种设备

认证