文件编号：CCRC-QOG-0436-B/1

软件安全开发服务资质认证

自评估表填写指南

发布/修订日期：2026 年 11 月 06 日

生效日期：2024 年 6 月 5 日

主控部门：服务认证中心

中国网络安全审查认证和市场监管大数据中心

填写要求：

1.当条款对应的需提供证明材料为制度或项目文档时，在“证明材料清单栏目”填写文档的完整名称。例如《XX 公司软件安全开发服务规范》、《XX 公司项目变更管理制度》、《XX 项目渗透测试方案》、《XX 项目需求分析报告》等，并概括地介绍制度或项目文档各章节的内容。

2.当条款对应的需提供证明材料为记录文档时，在“证明材料清单栏目”填写记录的完整名称。例如《XX 项目软件代码安全检查记录》、《XX 项目软件单元测试记录》、《XX 项目系统试运行记录》等，并概括地介绍记录文档的主要内容。

3.当条款对应的需提供证明材料为某制度或文档的某章节内容时，在“证明材料清单栏目”填写文档的完整名称及对应的章节编号。例如《XX 项目需求分析报告》第 X 章 安全性需求分析、《XX 项目概要设计说明书》第 X 章 安全设计等，并对相关内容进行总结概括。

4.所有出现在“证明材料清单”栏目中的文档，都需提供相应的电子版文档或纸质文档的扫描件作为证明材料，并按照条款的序号建立文件夹整理归档，建立文件夹的格式为“序号-条款的考核内容”，例如“1-软件开发服务流程”、“4-配置管理计划”、“31-试运行报告”等。

以下给出了一份填写样例，供申请组织进行参考。填报组织应按照填写样例的细粒度，进行相关信息的填报。当申请三级服务资质时，仅填写自评估表中与三级相关的条款（具体分两种情况：1、标明适用于三级的；2、未标明属于哪个级别的）；申请二级服务资质时，除填写标明适用于二级的条款之外，还应填写所有属于三级要求的条款；申请一级服务资质时，填写全部条款。

申请组织名称	XX 公司（全称）	申请级别	X 级
评估时间	XX 年 X 月 X 日-X 月 X 日	评估部门/人员	XX 部/XX

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	不适用	
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。				已制定《软件项目启动过程》（文件编号：XXX），2.3 节给出输入（软件项目方案申请表、项目估算记录、招标文件、投标文件、立项报告等），2.4 节给出输出（合同意向执行申请、软件项目启动通知、软件项目启动会议纪要等），第 3 节给出活动图（主要包含编写合同意向执行申请、审批合同意向执行申请、启动软件项目、下达项目任务书等过程）； 已制定《需求分析过程》（文件编号：XXX），2.3 节给出输入（用户需求说明书），2.4 节给出输出（项目日程、软件需求规格说明书、用户手册等），第 3 节给出活动图（主要包含制定详细日程、选择开发方法工具、项目估算等过程）； 已制定《系统设计过程》（文件编号：XXX），2.3 节给出输入（软件需求规格说明书），2.4 节给出输出（系统设计说明书、系统测试用例、集成测试用例等），第 3 节给出活动图（主要包含组织系统设计、编写集成测试用例、系统测试用例等过程）； 已制定《代码设计过程》（文件编号：XXX），2.3 节给出输入（系统设计说明书），2.4 节给出输出（单元测试用例、单元测试记录、重点代

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	不适用	
							码检查表等），第 3 节给出活动图（主要包含设计单元测试用例、编写模块代码、执行代码走查等过程）； 已制定《产品发布过程》（文件编号：XXX），2.3 节给出输入（系统设计说明书、模块源代码、用户手册、操作手册等），2.4 节给出输出（集成测试记录、缺陷跟踪、软件产品等），第 3 节给出活动图（主要包含搭建可运行环境、执行集成测试、整理手册、申请产品发布等过程）； 已制定《测试过程》（文件编号：XXX），2.3 节给出输入（系统测试用例、确认测试用例），2.4 节给出输出（系统测试用例记录、系统测试报告、确认测试报告、性能测试报告等），第 3 节给出活动图（主要包含建立测试环境、执行测试、编写测试报告等过程）； 已制定《系统实施过程》（文件编号：XXX），2.3 节给出输入（项目合同、用户需求说明书、软件产品等），2.4 节给出输出（培训资料、确认测试报告、培训签到表、用户问题跟踪表、系统验收申请、系统试运行报告、系统验收报告、项目总结报告等），第 3 节给出活动图（主要包含用户培训、系统试运行、系统验收等过程）。
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。				已制定 JAVA 编码规范、编码指南、软件编码规范等程序文件及规范。

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	不适用	
3.	准备阶段	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。				提供 XXX 项目开发计划，计划包含 XX、XX、XX 等章节内容，XX 章给出项目里程碑，XX 章对项目进度进行描述，XX 章对质量管控、沟通管理等进行描述。 备注：此条要求的安全要素可以体现在质量管控里面，例如代码的安全质量，也可以体现在其他方面。
4.		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。				提供 XX 项目配置管理计划，计划中包含 XX、XX 等章节内容，并对配置库权限等安全要求进行描述。
5.		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。				提供 XX 变更管理制度，制度包含 XX、XX、XX 等变更管理流程内容，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。 提供 XX 项目变更记录。
6.		**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。				提供项目风险管理制度，包含 XX、XX、XX 等内容。 提供 XX 项目风险分析报告，内容包含 XX、XX、XX 等。
7.	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				提供 XX 项目可行性报告/招标文件/需求分析报告，报告中 XX 章对软件功能需求进行描述，包含 XX、XX、XX 等功能；XX 章对软件性能需求进行描述，例如：并发数 100；XX 章对软件安全性需求进行描述，

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	不适用	
			等，需求文档的内容应涉及软件功能、性能及安全性要求。				包含审计、权限、单点登录、传输安全等安全功能需求。
8.		**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。	需求分析报告				提供 XXX 项目需求分析报告，报告包含 XX、XX、XX、XX 等主要章节内容。
9.		**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。					提供 XXX 项目需求分析报告，报告中 XX 章 XX 节包含软件开发所使用的安全技术标准或者规范，例如：GB/T 18336。
10.		**仅一级要求**：应基于软件安全威胁开展需求分析。					提供 XXX 项目需求分析报告，报告中 XX 章对 XX 单位 XX 应用目前所面临的威胁进行了分析，包含 XX、XX 等安全威胁，基于 XX、XX 安全威胁，提出了 XX、XX、XX 等安全需求。
11.		**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。					XX 项目使用 XX 安全开发模型，模型包含 XX、XX、XX 等主要过程要求，每个阶段均考虑安全因素，例如 XX 阶段需要进行 XXX 安全验证。
12.	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。				提供设计阶段控制程序文件，文件包含 XX、XX、XX 等内容。 提供 XX 项目设计说明书，包含 XX、XX、XX 等章节内容。
13.		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。					提供 XX 项目设计说明书，XX 章对 XX、XX、XX 等功能性设计进行了详细描述，XX 章对 XX、XX、XX 等非功能性设计进行了详细描述。

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	不适用	
14.		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。					提供 XX 项目设计说明书，XX 章包含 XX、XX、XX 等安全功能设计。
15.		**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。				提供 XX 项目概要设计说明书，XX 章包含 XX、XX、XX、XX 等安全功能设计。
16.		**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。					提供 XX 项目概要设计说明书，基于 XX 威胁，提出了 XX 设计；基于 XX 威胁，提出了 XX 设计。
17.		**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。					提供 XX 项目概要设计说明书，XX 章包含 CA、数字证书等安全功能设计。
18.		**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。				提供 XX 项目详细设计说明书，包含 XX、XX、XX、XX 等安全功能详细设计。

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	不适用	
19.		**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。					提供 XX 项目详细设计说明书，针对 XX 威胁，提出 XX 设计。
20.	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。				提供 XX、XX、XX 等安全编码规范，包含 XX、XX、XX 等安全编码规则。
21.		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。				提供 XX 项目软件代码安全检查/评审记录，提供有 XX、XX 漏洞的修复记录与验证结果记录。
22.		**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。				提供 XX 项目软件代码安全检查/评审记录，包含 XX、XX、XX 等安全检查内容。
23.		**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。				公司采用 XX 工具进行软件代码安全检查，提供有 XX 项目 XX 工具检查结果/报告。
24.	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。				提供 XX 项目测试方案，包含 XX、XX、XX 等内容。 提供 XX 项目测试计划，包含 XX、XX 等测试计划安排内容。 提供 XX 项目功能测试记录、安全测试记录。

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	不适用	
							提供 XX 项目测试报告，包含 XX、XX 等内容，测试结论为 XX、XX。
25.		对测试发现的漏洞进行分析并有效修复。	漏洞发现、分析与修复的记录。				提供 XX 测试记录/报告，其中包含发现的 XX 漏洞，XX 文档对 XX 漏洞进行了分析，提供 XX 漏洞修复记录，修复记录中包含修复结果。
26.		**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。				提供 XX 项目安全性测试计划，包含 XX、XX 等安全测试计划安排。 提供 XX 项目安全测试用例设计文档，包含 XX、XX、XX 等安全测试用例。 提供 XX 项目安全测试记录，包含 XX、XX、XX 等安全测试结果。
27.		**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。				提供 XX 项目脆弱性测试方案，包含 XX、XX、XX 等脆弱性测试方法。 提供 XX 项目脆弱性测试记录，包含 XX、XX、XX 等脆弱性测试结果。
28.		**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。				提供 XX 项目渗透测试方案，包含 XX、XX 等内容。 提供 XX 项目渗透测试记录，包含 XX、XX 等渗透测试过程记录。 提供 XX 项目渗透测试报告，包含 XX、XX、XX 等内容。
29.	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。				提供 XX 项目系统试运行记录，试运行开始日期：XX，结束日期：XX，试运行周期 XX。

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	不适用	
30.		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。				提供 XX 项目调整/维护记录，记录中包含对 XX、XX、XX 等问题更新维护记录。
31.		**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。				提供 XX 项目试运行报告，包含 XX、XX、XX 等内容。
32.		**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。				提供 XX 项目系统试运行记录，试运行开始日期：XX，结束日期：XX，试运行周期 XX。 提供 XX 项目试运行报告，包含 XX、XX、XX 等内容。
33.		**仅一级要求**：综合软件系统试运行状态，建立软件系统运行策略和安全指南。	系统运行策略、安全指南。				提供 XX 项目系统运行策略，包含 XX、XX、XX 等内容。 提供 XX 项目系统运行安全指南，包含 XX、XX、XX 等内容。
34.	验收阶段 - 验收交付	根据合同约定，进行项目验收，形成项目验收报告。	验收申请、验收资料、验收报告。				提供 XX 项目验收报告，验收日期：XX。
35.	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。				提供 XX 项目巡检记录，巡检内容包含 XX、XX、XX 等。 提供 XX 项目故障记录，包含 XX、XX 等故障记录。 提供 XX 项目升级更新记录，包含 XX、XX、XX 等问题更新升级记录。
36.		**仅二级/一级要求**：制定系	系统运行计划、安全事件响应				提供 XX 项目系统运行计划，包含 XX、XX、XX 等内容。

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	不适用	
		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。	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。				提供 XX 应急预案，XX 章对安全事件应急响应计划进行描述，XX 章对安全事件应急预案进行详细描述，XX 章包含应急保障团队人员构成，包含 XX、XX、XX 等人员。 提供 XX 项目应急事件记录，包含 XX、XX 等安全事件应急响应记录。
37.		**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。					提供 XX 项目 XX 安全事件应急响应报告，包含 XX、XX、XX 等内容。
38.		**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。				提供 XX 项目健康检查计划，包含 XX、XX 等内容。 提供 XX 项目健康检查记录。 提供 XX 项目健康检查报告，包含 XX、XX 等内容。 提供 XX 项目巡检报告，包含 XX、XX 等内容。
39.		**仅一级要求**：根据健康检查报告进行分析，持续优化系统。					提供 XX 项目系统优化改进记录，依据 XX 健康检查报告对出现的 XX、XX 等问题进行了优化改进。

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。