文件编号：CCRC-QOG-0439-B/0

渗透测试服务资质认证自评估表填写指南

发布/修订日期：2026 年 11 月 16 日

生效日期：2026 年 11 月 16 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

程序文件修改记录

序号	上一版本文件编码	修改章节	文件更改通知单编号	修改日期	修改人	批准人
1		新增		2026.11	段静辉	张斌

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 公司渗透测试服务规范》、《XX 项目渗透测试实施方案》、《XX 项目渗透测试报告》等，并概括地介绍制度或项目文档各章节的主要内容。

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《工具适用性测试记录》、《XX 项目人员培训记录》、《XX 项目专家评审意见》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 项目渗透测试服务实施方案》第 X 章 项目团队介绍、《XX 项目渗透测试服务评估报告》第 X 章信息收集分析等，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-服务流程”、“10-渗透测试调研报告”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		申请级别	
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	不适用	
1.	服务技术要求	建立渗透测试服务流程。	渗透测试服务流程图，图中应包括每个阶段对应的职责、输入输出等。				提供《渗透测试服务流程》（包含 XX 阶段、XX 阶段、XX 阶段、XX 阶段），对每个阶段的目标、角色、内容、输出进行了说明。 1.XX 阶段： 目标： 工作内容： 输出： ……
2.		制定渗透测试服务规范并按照规范实施。	渗透测试服务规范。				提供《渗透测试服务规范》，包含 XX、XX、XX、XX 等章节内容。
3.	渗透准备-需求调研	目标系统范围、业务类型、支持业务运行的系统技术框架和组件类型。	渗透测试调研计划或调研表等，能证明调研项目覆盖全部审核条款				提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含目标系统范围、业务类型、支持业务运行的系统技术框架和组件类型等内容。
4.		目标系统业务高峰、测试时间与周期					提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含目标系统业务高峰、测试时

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	
							间与周期等内容。
5.		目标系统是否有登录功能，如需登录测试，能否提供不同权限的测试账号。					提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含目标系统是否有登录功能及登录测试的相关记录等内容。
6.		渗透测试实施方式，如需远程测试，是否需要VPN，是否有防火墙、WAF设备，是否可加白名单					提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含渗透测试可以采取的实施方式等内容。
7.		目标系统负责人、对接人、应急联系人的联系方式。					提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含目标系统负责人、对接人、应急联系人的联系方式。
8.		**仅二级/一级要求：**渗透测试限制条件和注意事项	针对本次渗透测试的限制条件和注意事项的说明文档				提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》，包含渗透测试限制条件和注意事项。
9.	渗透准备-需求确认	形成覆盖全部调研内容的调研记录，包括但不限于系统名称、业务类型、功能介绍、联系人等	渗透测试调研记录等记载具体调研内容的文档				提供 XX 项目的《渗透测试项目调研计划》或《渗透测试项目调研表》。
10.		**仅二级/一级要求：**编制渗透测试调研报告	渗透测试调研报告，相对调研记录应增强对需求的具体分析及详细策略等细化报告。				提供 XX 项目的《渗透测试调研报告》，包含 XX、XX、XX、XX 等章节内容。
11.	渗透准备-方案制定	项目概述、服务背景、测试范围、测试原则、组织架构等	渗透测试方案，方案具体内容应覆盖全部审核条款。				提供 XX 项目的《渗透测试方案》，包含 XX、XX、XX、XX 等章节内容。

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	
12.		测试对象、测试时间、测试方式（黑盒、灰盒、白盒）、测试接入方式（互联网、内网、专网）、测试计划、签订保密协议、工具准备等					提供 XX 项目的《渗透测试方案》，包含测试对象、测试时间、测试方式（黑盒、灰盒、白盒）、测试接入方式（互联网、内网、专网）、测试计划、签订保密协议、工具准备等内容。
13.		实施流程、测试授权、信息收集、漏洞测试、测试收尾、项目验收等					提供 XX 项目的《渗透测试方案》，包含实施流程、测试授权、信息收集、漏洞测试、测试收尾、项目验收等内容。
14.		调研记录、渗透测试记录与报告等项目交付物					提供 XX 项目的《渗透测试方案》，包含调研记录、渗透测试记录与报告等项目交付物等内容。
15.		项目实施风险及规避措施等。					提供 XX 项目的《渗透测试方案》，包含项目实施风险及规避措施等内容。
16.	渗透准备-方案确认	获得委托方对渗透测试方案的确认，确认方式可选择通过邮件、会议纪要、签字等任意一种方式。	由客户出具的方案确认材料。				提供 XX 项目的方案确认材料，可以是邮件、会议纪要、签字等。
17.	渗透实施-渗透测试授权	获得委托方的书面授权，授权书应签字或加盖单位公章。授权书内容包括但不限于委托方名称、联系人姓名、联系电话、允许测试时间、渗透测试范围（URL/IP/系统）、双方声明。	由客户出具的本次渗透测试书面授权材料。				提供 XX 项目的《渗透测试授权书》等材料。

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	
18.	渗透实施-信息收集分析	对目标系统所在服务器端口的开放情况进行探测	记录探测过程及结果的相关日志或报告等材料。				提供对 XX 项目的目标系统所在服务器端口的开放情况进行探测的过程及结果的相关日志或报告等材料。
19.		对目标系统业务功能进行分析，识别出关键功能模块、关键功能接口以及业务流程等，并对识别的资产进行信息收集及分析，包括但不限于Web网站、APP客户端、小程序等资产。	记录分析识别到功能模块、接口等资产的日志或报告等材料。				提供对 XX 项目的目标系统业务功能实施分析的材料。
20.		**仅二级/一级要求**：通过对目标系统的信息收集，识别目标系统前端、后端、以及系统架构、通用组件、数据库类型、通信方式、加密特征等关键信息；	记录关键信息的报告、拓扑图等材料				提供对 XX 项目的目标系统的信息收集和识别的材料
21.		**仅二级/一级要求**：通过结合目标系统特征，关联进行信息收集，包括关联源码信息、系统版本号、系统弱口令、网盘等；					提供对 XX 项目结合目标系统特征，关联进行信息收集的材料
22.		**仅二级/一级要求**：对收集到的资产、业务特征、系统架构、关联资产信息的整合分析。					提供对 XX 项目收集的资产、业务特征、系统架构、关联资产信息整合分析的证明材料
23.		**仅一级要求**：利用第三方工具或威胁情报平台等方式方法，对目标系统进行全面的敏感信息收集；	第三方工具的使用截图、日志或报告等材料				提供对 XX 项目使用第三方工具或威胁情报平台收集信息的过程截图、日志或报告等材料

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	
24.		**仅一级要求：**通过一定的自动化开发工作，编写自动化信息收集工具，对目标系统的暴露面进行信息收集。	简单演示自动化工具，提供自动化工具的相关日志或操作记录等材料				提供对 XX 项目自动化工具的相关日志或操作记录等材料，现场简单演示自动化工具使用
25.	渗透实施-漏洞发现	利用收集到的信息，使用漏洞扫描工具进行漏洞扫描	漏扫工具清单、漏扫工具截图、漏扫报告及日志等材料				提供漏扫工具清单 提供对 XX 项目使用漏扫工具收集信息的截图、漏扫报告及日志等材料
26.		利用收集到的信息，通过人工方式识别漏洞，并进行针对性漏洞挖掘。	漏洞发掘报告等材料				提供 XX 项目漏洞发掘报告
27.		**仅二级/一级要求**：通过对系统输入不同的数据和命令，使用黑盒漏洞发现方法，发现潜在漏洞。	提供详细描述发现过程的漏洞报告和相应截图				提供 XX 项目漏洞报告和相应截图
28.		**仅一级要求：**通过访问系统源代码、配置文件和文档等信息，使用白盒漏洞发现方法，发现潜在漏洞	提供详细描述发现过程的漏洞报告和相应截图				提供 XX 项目漏洞报告和相应截图
29.		**仅一级要求：**通过对系统输入大量的随机、异常或非预期的数据，使用模糊测试方法，发现系统潜在漏洞。	提供详细描述发现过程的漏洞报告和相应截图				提供 XX 项目漏洞报告和相应截图
30.	渗透实施-漏洞验证	针对被测目标系统进行漏洞利用和验证,并结合业务情况描述漏洞影响	记录漏洞利用过程和漏洞验证的报告及漏洞验证、后门清理的操作日志等				提供 XX 项目漏洞利用过程和漏洞验证的报告及漏洞验证、后门清理的操作日志等
31.		应在测试过程中，针对增加、删除、修改、查询等测试动作进行记录，并在测试结束后，协助委托方进行后门清理、					提供 XX 项目漏洞利用过程和漏洞验证的报告及漏洞验证、后门清理的操作日志等

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	
		痕迹清除等工作。					
32.		**仅二级/一级要求**：在测试过程中，确保测试范围完整和风险可控，并保留测试过程中能够证明漏洞存在的关键截图、记录漏洞发生的参数位置信息及功能模块、记录漏洞验证的详细条件及验证过程	记录漏洞详细信息的报告、截图、操作日志等的相关材料				提供 XX 项目漏洞详细信息的报告、截图、操作日志等的相关材料
33.		**仅二级/一级要求**：通过自动化手段对目标系统存在漏洞进行验证和分析	自动化工具清单、自动化工具使用截图、操作日志和报告等材料				提供 XX 项目自动化工具清单、使用自动化工具验证和分析的目标系统漏洞的截图等材料
34.		**仅二级/一级要求**：尝试通过多个漏洞的关联利用验证漏洞的综合可利用性及可能造成的实质影响	记录关联利用多个漏洞的报告				提供 XX 项目关联利用多个漏洞的报告
35.		**仅一级要求：**能够持续进行原创漏洞挖掘和验证，具备CNNVD、CNVD任意证书的相应证明材料。	记录漏洞挖掘的相关报告、相关漏洞平台提交记录及相关证书				提供 CNNVD、CNVD 任意证书。
36.	渗透实施-漏洞评价	参考国家标准，并结合行业相关标准，确定漏洞评价准则；	描述漏洞评价标准的规范性文件				提供 XX 项目的《渗透测试报告》，包含漏洞评价准则等内容。
37.		对漏洞风险进行定级和统计	描述漏洞风险定级规则的规范性文件				提供 XX 项目的《渗透测试报告》，包含漏洞风险进行定级和统计等内容。
38.		**仅二级/一级要求**：对已定级漏洞，根据业务场景变化，再次评估影响范围、	描述针对影响范围、利用难度等具有针对性的定级算法的规范性文件、具				提供 XX 项目的《渗透测试报告》，包含根据业务场景变化，再次评估影响范围、利用难度，修订漏洞等

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	
		利用难度，修订漏洞等级	体漏洞级别计算和修订记录				级等内容。
39.		**仅二级/一级要求**：已发现的漏洞类型未在漏洞评价准则中给予说明的或漏洞等级与漏洞定级评价准则存在出入的，应给出漏洞级别修订的原因，并完善本项目的漏洞评价准则。	本项目的针对性漏洞评价准则及修订原因相关规范性文件				提供 XX 项目的《渗透测试报告》，如存在已发现的漏洞类型未在漏洞评价准则中给予说明的或漏洞等级与漏洞定级评价准则存在出入的，包含漏洞评价准则和漏洞级别修订等内容。
40.	渗透总结-报告编制	摘要、正文、版本信息、商业秘密等级（根据系统属性确定）	渗透测试总结性报告文件，包括明确工作内容、过程、方法、文档模板，内容应覆盖审核条款的要求。				提供 XX 项目的《渗透测试报告》，包含摘要、正文、版本信息、商业秘密等级等内容。
41.		渗透测试目标、范围、时间、工具、人员；					提供 XX 项目的《渗透测试报告》，包含目标、范围、时间、工具、人员等内容。
42.		漏洞评价准则；					提供 XX 项目的《渗透测试报告》，包含漏洞评价准则等内容。
43.		测试过程中发现所有漏洞及修复建议等					提供 XX 项目的《渗透测试报告》，包含漏洞清单及对应的修复建议等内容。
44.		**仅二级/一级要求**：详细记录测试的技术细节和发现的问题	渗透测试总结性报告中应包含详细的测试步骤描述、截图附件、统计性和分析性结论和整体安全评价。				提供 XX 项目的《渗透测试报告》，包含详细的测试步骤描述、截图附件等内容。
45.		**仅二级/一级要求**：测试目标的漏洞统计数据和整体风险情况总结及安全评价。					提供 XX 项目的《渗透测试报告》，包含基于发现漏洞的统计性和分析性结论和整体安全评价等内容。
46.		**仅一级要求**：对未公开信息或未发布补丁的漏洞提出缓解措施；	渗透测试总结性报告中如有未公开信息或未发布补丁的漏洞，应提供可				提供 XX 项目的《渗透测试报告》，如存在未公开信息或未发布补丁的漏洞，包含针对性的缓解措施等内

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	
			落地有针对性的风险降低措施。				容。
47.		**仅一级要求**：对潜在的业务影响进行分析，根据渗透测试的结果和发现的漏洞，评估潜在的业务影响，包括数据泄露、服务中断、信息篡改等，提供对业务的风险评估和建议。	渗透测试总结性报告中应明确描述漏洞导致的潜在业务影响，包括数据泄露、服务中断、信息篡改等，提供对业务的风险评估和建议				提供 XX 项目的《渗透测试报告》，包含由于漏洞导致的数据泄露、服务中断、信息篡改等潜在业务影响及风险评估和建议等内容。
48.	渗透总结-报告评审交付	对渗透测试报告进行内部评审，并得到委托方确认	加盖了公章、法人签字、数字签名等印章的渗透测试报告 渗透测试报告内部评审记录、委托方出具的评审报告或验收报告 渗透测试报告交付时的保障措施记录				提供 XX 项目的《渗透测试报告》，报告已加盖公章、法人签字、数字签名等。
49.		向委托方交付加盖公章或其他具有法律效力的印章的渗透测试报告，并采取措施保证报告交付的机密性和完整性。					提供 XX 项目的《渗透测试报告评审记录》 提供单位的渗透测试报告交付的管理要求，及交付的保障措施记录
50.	渗透总结-漏洞复测	具备漏洞复测的能力	根据合同，如有漏洞复测要求，提供漏洞复测记录或日志等证明文件				提供 XX 项目的《漏洞复测记录》或《工作日志》等材料
51.		根据合同需要，进行漏洞复测					提供 XX 项目的《漏洞复测记录》或《工作日志》等材料
52.		**仅二级/一级要求**：提供漏洞复测报告	提供完整的漏洞复测报告，应与渗透测试漏洞报告匹配				提供 XX 项目的《漏洞复测报告》等材料