信息安全风险评估服务资质认证自评估表填写指南

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 公司信息安全风险评估服务规范》、《XX 项目信息安全风险评估实施方案》、《XX 公司风评工具管理制度》、《XX 项目资产清单》、《XX 项目信息安全风险评估报告》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 项目信息安全风险评估实施方案》第 X 章 项目团队介绍、《XX 项目信息安全风险评估报告》第 X 章 脆弱性分析等，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”、“6-挖掘漏洞信息”、“13-风险评估工具”、“32-已有安全措施分析”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。

组织名称	XX 公司（全称）	申报级别	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	
1.	服务技术要求	建立信息安全风险评估服务流程。	按照相关标准建立的信息安全风险评估服务流程，流程图中应包括每个阶段对应的职责、输入输出等。			提供《信息安全风险评估服务流程》（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.		制定信息安全风险评估服务规范并按照规范实施。	已制定的信息安全风险评估服务规范。			提供《XX 公司风险评估服务规范》，包含 XX、XX、XX、XX 等章节内容。
3.	基本资格	**仅三级要求：**至少有一个完成的风险评估项目，该系统的用户数在 1,000 以上； 具备从管理或（和）技术层面对脆弱性进行识别的能力。	一个已完成项目的合同、用户数、验收的证明材料，包括管理或（和）技术层面脆弱性识别的材料。			项目名称： 系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额：
4.		**仅二级要求：**针对多种类型组织，多行业组织，至少完成一个风险评估项目，	一个已完成项目的合同、用户数、验收的证明材料，包括管理和技术层面			项目名称： 行业类型：

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	
		该系统的用户数在 10,000 以上；具备从管理和技术层面对脆弱性进行识别的能力。	脆弱性识别的材料。			系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额：
5.		**仅一级要求：**能够在全国范围内，针对 5 个（含）以上行业开展风险评估服务；至少完成两个风险评估项目，该系统的用户数在 100,000 以上；具备从业务、管理和技术层面对脆弱性进行识别的能力。	5 个已完成项目的合同、用户数、验收的证明材料，从业务、管理和技术层面对脆弱性进行识别的材料。			1.项目名称： 行业类型： 系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额： 2.项目名称： 行业类型： 系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额： 3.项目名称： 行业类型： 系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额：

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	
						4.项目名称： 行业类型： 系统规模（用户数）： 合同签订时间： 项目验收时间： 合同金额： 5.项目名称： 行业类型： 系统规模（用户数）： 合同签订时间：
6.		**仅一级要求：**具备跟踪、验证、挖掘信息安全漏洞的能力。	跟踪、验证、挖掘信息安全漏洞的证明材料。			提供公司近 X 年提交的漏洞信息： CNNVD-201510-XXX 提交人：XX CNNVD-201510-XXX 提交人：XX CNNVD-201603-XXX 提交人：XX
7.	准备阶段-服务方案制定	编制风险评估方案、风险评估模板，并在项目实施过程中按照模板实施。	信息安全风险评估方案、风险评估模板。			提供 XX 项目的《风险评估项目实施方案》，包含 XX、XX、XX、XX 等章节内容。 提供《风险评估实施方案模板》、包含 XX、XX、XX、XX 等章节内容， 提供《风险评估报告模板》，包含 XX、XX、XX 等章节内容。
8.		应为风险评估实施活动提供总体计划或方案，方案应包含风险评价原则。	已完成项目的风险评估方案，方案中应包含风险评价原则。			提供 XX 项目的《风险评估项目实施方案》，在 XX 章节，对风险评估理论模型、评估原则和方式进行了明确，风

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	
						险评价原则为……
9.		**仅二级/一级要求：**应进行充分的系统调研，形成调研报告。	已完成项目的系统调研报告，报告中对被评估对象有清晰的描述。			提供 XX 项目的《需求调研报告》，包含 XX、XX、XX 等章节内容。
10.		**仅二级/一级要求：**宜根据风险评估目标以及调研结果，确定评估依据和评估方法。	已完成项目的风险评估实施方案中应根据目标及调研结果，明确评估依据和评估方法，评估依据和评估方法符合国家标准、行业标准及相关要求。			提供 XX 项目的《风险评估项目实施方案》，在 XX 章节能够对风险评估依据的标准和评估方法进行明确，评估标准主要包括 XX、XX、XX 等。
11.		**仅二级/一级要求：**应形成较为完整的风险评估实施方案。				提供 XX 项目的《风险评估项目实施方案》。
12.	准备阶段-人员和工具管理	应组建评估团队。风险评估实施团队应由管理层、相关业务骨干、IT 技术人员等组成。	已完成项目的风险评估方案中对风险评估实施团队成员及团队构架的介绍。			提供 XX 项目的《评估团队组成》文档，对评估组的组织架构和人员进行了明确，包括 XX、XX、XX 等角色，并对项目组成员的资质进行了介绍。
13.		应根据评估的需求准备必要的工具。	已完成项目的风险评估方案中对评估工具的介绍，工具列表及主要功能描述。			提供 XX 项目的《风险评估工具》文档，对该项目涉及到的评估工具进行了明确，包括 XX、XX、XX，对工具的主要功能进行了介绍。
14.		应对评估团队实施风险评估前进行安全教育和技术培训。	项目实施前的安全教育及技术培训的证明材料，如启动会的 PPT，PPT 中包含培训的内容。			提供 XX 项目的《项目启动 PPT》，对项目的 XX、XX、XX 等内容进行了介绍,以及其他可证明对其安全教育、技术方面培训的材料。
15.		**仅二级/一级要求：**需采取相关措施，保障工具自身的安全性、适用性。	工具的安全测试证明材料；定期或工具软件有重大版本变更时，对工具软件进行适用性确认的测试记录。			提供《安全服务项目实施工具更新记录表》，包括 XX、XX、XX 等信息，对工具定期进行策略更新。
16.		**仅一级要求：**需采取相关措施，保障工	已制定的工具管理制度及执行记录。			提供《工具管理办法》，包含 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	
		具管理的规范性。				
17.	风险识别阶段-资产识别	参考国家或国际标准，对资产进行分类。	参照已发布的标准，形成的资产分类列表。			提供《风险评估实施规范》，其中在 X 章节对资产的分类标准进行了明确，共分为 XX、XX、XX、XX 等几种。
18.		识别重要信息资产，形成资产清单。	已完成项目的重要资产清单。			提供 XX 项目的《重要资产清单》。
19.		对已识别的重要资产，分析资产的保密性、完整性和可用性等安全属性的等级要求。	已完成项目的重要资产的三性等级要求列表。			提供 XX 项目的《资产赋值-硬件资产》、《资产赋值-软件资产》、《资产赋值-数据资产》文档，能够分析资产 XX、XX、XX 等安全属性的等级要求。
20.		对资产根据其在保密性、完整性和可用性上的等级分析结果，经过综合评定进行赋值。	已完成项目的重要资产赋值表。			提供 XX 项目的《资产赋值-硬件资产》、《资产赋值-软件资产》、《资产赋值-数据资产》文档，能够体现重要资产的赋值结果。
21.		**仅一级要求：**识别信息系统处理的业务功能，重点识别出关键业务功能和关键业务流程。	已完成项目中识别信息系统、以及业务系统承载的业务、业务流程的证明材料。			提供 XX 项目的《关键业务功能和关键业务流程分析文档》，识别的关键业务功能为 XX，识别的关键业务流程为 XX。
22.		**仅一级要求：**根据业务特点和业务流程识别出关键数据和关键服务。	已完成项目中识别信息系统、以及业务系统承载的业务、业务流程的证明材料。			提供 XX 项目的《关键业务功能和关键业务流程分析文档》，关键业务流程 XX 依托的关键数据为 XX，依托的关键服务为 XX。
23.		**仅一级要求：**识别处理数据和提供服务所需的关键系统单元和关键系统组件。	已完成项目中对处理数据和提供服务所需的关键系统单元和关键系统组件的识别分析证明材料。			提供 XX 项目的《关键业务功能和关键业务流程分析文档》，处理数据和提供服务所需的关键系统单元为 XX，关键系统组件为 XX。
24.	风险识别阶段-脆弱	应对已识别资产的安全管理或技术脆弱性利用适当的工具进行核查，并形成	已完成项目中对脆弱性识别时使用的工具列表、管理或技术脆弱性列			提供 XX 项目的《安全管理脆弱性检查表》，及物理、网络、主机、数据库的技术脆弱性检查表。

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	
	性识别	安全管理或技术脆弱性列表。	表。			
25.		应对脆弱性进行赋值。	已完成项目的脆弱性赋值列表。			提供 XX 项目的《硬件资产脆弱性赋值结果》、《软件资产脆弱性赋值结果》、《数据资产脆弱性赋值结果》、《管理脆弱性赋值结果》文档。
26.	风险识别阶段-威胁识别	应参考国家或国际标准，对威胁进行分类；	威胁分类清单。			提供《风险评估实施规范》，其中在 X 章节对威胁的分类方法进行了明确，共分为 XX、XX、XX、XX 等。
27.		应识别所评估信息资产存在的潜在威胁；	已完成项目中的威胁识别清单。			提供 XX 项目的《威胁分析报告》、《威胁赋值表》，识别出的信息系统面临的威胁类型主要包括 XX、XX、XX、XX 等类型。
28.		应识别威胁利用脆弱性的可能性；	已完成项目中分析威胁利用脆弱性可能性的证明材料。			提供 XX 项目的《硬件资产风险计算结果》、《软件资产风险计算结果》、《数据资产风险计算结果》、《管理风险计算结果》文档，能够将威胁和脆弱性进行关联，评价威胁利用脆弱性的可能性。
29.		应分析威胁利用脆弱性对组织可能造成的影响。	已完成项目中分析脆弱性发生对组织造成影响的证明材料。			提供 XX 项目的《硬件资产风险计算结果》、《软件资产风险计算结果》、《数据资产风险计算结果》、《管理风险计算结果》文档，能够将资产价值和脆弱性进行关联，评价所评估资产的脆弱性一旦被威胁利用所造成的影响。
30.		**仅二级/一级要求：**应识别出组织和信息系统中潜在的对组织和信息系统造成影响的威胁。	已完成项目中对组织和信息系统造成的潜在威胁进行分析的证明材料。			提供 XX 项目的《威胁分析报告》、《威胁赋值表》，其中，来自组织和信息系统内部的威胁主要包括 XX、XX、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	
31.		**仅一级要求：**采用多种方法进行威胁调查。	已完成项目中采取多种威胁调查方法的证明材料。			提供 XX 项目的《安全威胁调研问卷》、《威胁分析报告》，采用的威胁调查方法包括 XX、XX、XX 等。
32.	风险识别-已有安全措施确认	应识别组织已采取的安全措施；	已完成项目中的已识别的安全措施列表。			提供 XX 项目的《安全措施描述表（技术）》、《安全措施描述表（管理）》，对被评估信息系统的安全措施进行识别。
33.		应评价已采取的安全措施的有效性。	已完成项目中分析安全措施有效性的证明材料。			提供 XX 项目的《安全措施有效性分析表》。
34.	风险分析阶段-风险分析模型建立	应构建风险分析模型。	已完成项目的风险评估报告中对风险分析模型的描述，并验证其可行性、科学性。			提供 XX 项目的《项目实施方案》，以及《信息安全风险评估报告》，在 XX 章节，对风险评估框架和计算模型进行了明确，风险计算模型为 XX。
35.		应根据风险分析模型对已识别的重要资产的威胁、脆弱性及安全措施进行分析。	已完成项目的风险评估报告中，对威胁、脆弱性及安全措施分析的描述。			提供 XX 项目的《信息安全风险评估报告》，其中在 X 章节体现了脆弱性识别、威胁识别、安全措施有效性分析的内容。
36.		应根据分析模型确定的方法计算出风险值。	已完成项目的风险评估报告中对风险计算方法的描述，计算得出风险值的过程。			提供 XX 项目的《硬件资产风险计算结果》、《软件资产风险计算结果》、《数据资产风险计算结果》、《管理风险计算结果》文档。
37.		**仅二级/一级要求：**构建风险分析模型应将资产、威胁、脆弱性三个基本要素及每个要素各自的属性进行关联。	已完成项目的风险评估报告中对资产、威胁、脆弱性三个基本要素进行关联的证明材料。			提供 XX 项目的《硬件资产风险计算结果》、《软件资产风险计算结果》、《数据资产风险计算结果》、《管理风险计算结果》文档，能将资产、威胁、脆弱性三个基本要素进行关联，最终风险值参考资产、脆弱性、威胁的赋值计算得出。

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	
38.	风险分析阶段-风险计算方法确定	**仅二级/一级要求：**在风险计算时，应根据实际情况选择定性计算方法或定量计算方法。	已完成项目的风险评估报告中的计算方法。			XX 项目采用 XX 计算方法。
39.	风险分析阶段-风险评价	应根据风险评价准则确定风险等级。	已完成项目的风险评估报告中的评价准则，并根据评价准则确定风险等级的证明材料。			提供 XX 项目的《硬件资产风险计算结果-等级化处理》、《软件资产风险计算结果-等级化处理》、《数据资产风险计算结果-等级化处理》、《管理风险计算结果-等级化处理》文档。
40.		**仅二级/一级要求：**应对不同等级的安全风险进行统计、评价，形成最终的总体安全评价。	已完成项目的风险评估报告中的安全评价内容。			提供 XX 项目的《信息安全风险评估报告》，在 XX 章节对不同等级的安全风险进行统计、评价，形成最终的总体安全评价为……
41.	风险分析-风险评估报告	应向客户提供风险评估报告。	已完成的所申请资质级别要求数量的风险评估报告。			提供 XX 项目的《信息安全风险评估报告》。
42.		报告应包括但不限于评估过程、评估方法、评估结果、处置建议等内容。	已完成的所申请资质级别要求的风险评估报告，报告中至少包括评估过程、评估方法、评估结果、处置建议等内容。			提供 XX 项目的《信息安全风险评估报告》，包括 XX、XX、XX、XX 等章节内容，与 XX 公司《信息安全风险评估报告模板》内容一致。
43.		**仅二级/一级要求：**风险评估报告中应对本次评估建立的风险分析模型进行说明，并应阐明本次评估采用的风险计算方法及风险评价方法。	2-3 份报告中对评估模型、评估方法、评价方法等描述的内容。			提供 XX 项目的《信息安全风险评估报告》，第 X 章节对风险评估分析模型进行了描述，所采用的风险计算方法为……，所采用的风险评价方法为……

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	
44.		**仅二级/一级要求：**风险评估报告中应对计算分析出的风险给予比较详细的说明。	已完成项目的风险评估报告中对风险给予详细说明的证明材料。			提供 XX 项目的《信息安全风险评估报告》，在 X 章节对风险给予详细说明。
45.	风险处置阶段-风险处置原则确定	**仅二级/一级要求：**应协助被评估组织确定风险处置原则，以及风险处置原则适用的范围和例外情况。	已完成项目的风险评估报告或建议报告中对风险处置原则及适用的范围和例外情况说明的证明材料。			提供 XX 项目的《信息安全风险评估报告》，在 X 章节对风险处置原则进行了明确，风险处置原则为……
46.	风险处置阶段-安全整改建议	**仅二级/一级要求：**对组织不可接受的风险提出风险处置措施。	已完成项目的风险评估报告或建议报告中对组织不可接受的风险提出风险处置措施或建议的证明材料。			提供 XX 项目的《风险处置计划》，针对不可接受风险提出了 XX、XX、XX 等处置措施。
47.	风险处置阶段-组织评审会	**仅一级要求：**协助被评估组织召开评审会。	服务提供者协助被评估组织组织评审会的证明材料，如会议通知、专家签到表、专家意见等。			提供 XX 项目的验收材料，有客户公司负责人对风险评估项目的验收意见及签字确认。
48.		**仅一级要求：**依据最终的评审意见进行相应的整改，形成最终的整改材料。	已完成项目的专家评审意见、整改措施及其总结。			提供 XX 项目的《风险评估整改材料》，对专家提出的 XX、XX 问题进行了整改（或者 XX 项目未涉及到需要整改的情形）。
49.	风险处置阶段-残余风险处置	**仅一级要求：**对组织提出完整的风险处置方案。	已完成项目的残余风险处置方案，方案至少包含处置措施、工具、时间计划等内容。			提供 XX 项目的《风险处置计划》，针对不可接受风险提出了 XX、XX、XX 等处置措施。
50.		**仅一级要求：**必要时，对残余风险进行再评估。	已完成项目中对残余风险进行再评估的证明材料。			提供 XX 项目的《残余风险评估报告》，对 XX、XX、XX 等残余风险进行了再评估，评估结果为……

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	
51.	上一年度提出的观察项整改情况（如有）					
52.		XXXX（描述前一年度观察项）				提供观察项整改措施、以及整改措施在新项目中的落实情况
53.						
54.	上一年度提出的不符合项整改情况（如有）					
55.		XXXX（描述前一年度不符合项）				提供不符合项整改措施，以及整改措施在新项目中的落实情况
56.						

自评估结论：

经自主评估，本单位的信息安全风险评估服务满足《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。