网络安全审计服务资质认证自评估表

填表要求：该服务中涉及的程序文件，须经本单位批准并发布。

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	建立网络安全审计服务流程。	提供建立的网络安全审计服务流程，流程中应包括每个阶段对应的职责、输入输出等。			
2.		制定网络安全审计服务规范并按照规范实施。	提供已制定的网络安全审计服务规范。			
3.	基本资格	**三级初次认证无项目要求。** **三级监督要求：**申请三级资质认证的单位，至少已经完成1个完整的网络安全审计项目，具备确定审计目标和范围、确定审计依据的能力；具备实施现场审计、报告审计发现和形成审计结论的能力；具备提出审计建议的能力。	提供一个已完成的审计项目的合同、验收的证明材料，包括确定审计目标和范围、确定审计依据的能力；实施现场审计、报告审计发现和形成审计结论的能力；提出审计建议的能力的证明材料。			
4.		**仅二级要求：**申请二级资质认证的单位，至少完成 **6 个完整的网络安全审计项目**；具备确定审计目标和范围、确定审计依据的能力；具备实施现场审计、报告审计发	提供 6 个已完成的审计项目的合同、验收的证明材料，包括确定审计目标和范围、确定审计依据的能力；实施现场审计、报告审计发现			

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	
		现和形成审计结论的能力；具备提出审计建议的能力。	和形成审计结论的能力；提出审计建议的能力的证明材料。			
5.		**仅一级要求：**申请一级资质认证的单位，至少完成 **10 个项目，3 个完整的网络安全审计项目**，项目审计目标应覆盖至少合规、安全、绩效等；具备确定审计目标和范围、确定审计依据的能力；具备实施现场审计、报告审计发现和形成审计结论的能力；具备提出审计建议的能力。	提供 3 个完整的网络安全审计项目的合同及验收的证明材料，项目审计目标应覆盖至少合规、安全、绩效等；包括确定审计目标和范围、确定审计依据的能力；实施现场审计、报告审计发现和形成审计结论的能力；提出审计建议的能力的证明材料。			
6.	**审计对象识别-了解被审计方业务和 IT 情况**	**G1.1.1** a) 编制业务情况调研表，并按照调研表收集有效信息。	提供业务情况调研表			
7.		**G1.1.1** b) 编制IT情况调研表，并按照调研表收集有效信息。	提供 IT 情况调研表			
8.		**（适用于一、二级）G2.1.1 a)** 编制审计对象列表，包括审计对象的数量、容量、功用、版本等属性。	提供审计对象列表，应包括审计对象的数量、容量、功用、版本等属性			
9.		**（适用于一、二级）G2.1.1** b) 梳理被审计方业务逻辑、应用系统处理逻辑和IT基础设施架构。	提供被审计方业务逻辑、应用系统处理逻辑和 IT 基础设施架构的分析证明材料			
10.		**（适用于一级）**G3.1.1 a) 应利用应用系统工具来建立和管理审计对象库。	提供利用应用系统工具建立和管理审计对象库的过程证明（可提供相关工具的功能介绍、界面截图等）			
11.		**（适用于一级）**G3.1.1 b) 具备为被审计方提供审计对象管理工具的能力。				
12.	**审计对象**	**G1.1.2 a) 有效掌握**被审计方组织结构。	提供了解和分析被审计方组织结			

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	
	调研-了解被审计方组织管理和IT管理情况		构及岗位职责等方法说明，如调研表等。			
13.		**G1.1.2 b)有效掌握**被审计方IT管理情况。	提供了解和分析被审计方 IT 管理情况的方法说明，如调研表等。			
14.		**G1.1.2 c)** 了解被审计方IT支撑业务的对应关系。	提供了解和分析被审计方 IT 支撑业务的对应关系说明，如分析表格模板。			
15.		**G1.1.2** d)对网络安全审计的风险进行初步评价。	提供网络安全审计风险评价方法，如评价程序，评价报告模板等。			
16.		**（适用于一、二级）G2.1.2** a) 梳理被审计方规章制度文件，形成审计项并编制对应检查表。	提供规章制度文件审计项及检查表模板及案例。			
17.		**（适用于一、二级）G2.1.2** b) 编制完整审计调研报告，并说明审计重点审计项。	提供审计调研报告案例，并说明审计重点审计项。			
18.		**G2.1.2 c)** 制定审计风险评价准则，评价审计风险，为确定重点审计项和明确审计内容提供依据。	提供审计风险评价准则，提供审计风险评价报告案例。			
19.		**（适用于一级）G3.1.2** 应建立审计调研报告分级复核程序，明确规定各级复核人员的要求和责任。	提供所建立的审计调研报告分级复核程序，明确规定各级复核人员的要求和责任。提供复核记录案例。			
20.	编制审计实施方案-确定网络	**G1.2.1** a）确定网络安全审计项目的目标。	提供确定审计目标的方法，如审计目标描述模板等。			
21.		**G1.2.1** b)网络安全审计目标可以包括信息化政策合规性、网络安全建设和绩效、				

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	
	安全审计目标	政务系统整合和数据共享、个人信息保护和数据保护、信息化项目建设绩效与合规、信息系统有效性和可靠性、信息系统应急响应能力等。				
22.		**（适用于一、二级）G2.2.1** 网络安全审计目标应经过评审，并与被审计方达成一致。	提供网络安全审计目标评审记录案例。			
23.	编制审计实施方案-确定网络安全审计依据	**G1.2.2 a）** 应根据具体审计目标，准确确定审计依据。	提供确定审计依据的方法，如审计目标与审计依据对应关系表格模板等。			
24.		**G1.2.2 b）**网络安全审计依据可以是国家法律法规、国际国内相关标准、被审计方的有关规章程序，以及审计委托方指定的其它审计依据。				
25.		**（适用于一、二级）G2.2.2** 应建立并维护常用审计依据库，并确保审计依据是当前适用版本。	提供审计依据库目录，并提供审计依据版本管理的方法。			
26.		**（适用于一级）G3.2.2** a) 应利用应用系统工具来建立和维护常用审计依据库，并确保审计依据是当前适用版本。	提供利用应用系统工具建立和维护审计依据库的过程证明（可提供相关工具的功能介绍、界面截图等）			
27.		**（适用于一级）G3.2.2** b) 具备为被审计方提供审计依据管理工具的能力。				
28.	编制审计实施方案-确定网络安全审计	**G1.2.3** a) 应根据审计目标和审计依据，确定审计范围。审计范围应包括组织机构范围、业务范围、IT 基础设施和应用系统范围等。	提供确定审计范围的方法，如审计目标、审计依据和审计范围的对应关系表格模板等。			

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	
29.	范围和审计内容	**G1.2.3** b)应根据审计依据和范围，确定审计内容。审计内容应划分到具体审计事项，明确每一个审计事项的审计要点和审计方法及所需资源。	提供确定审计内容的方法，如审计依据、审计范围和审计内容的对应关系表格模板。			
30.		G1.2.3 c） 审计方法及所需资源应包括审计人员、计划时间安排、审计工具，以及可操作的审计方法和流程。	提供不同审计内容对应的审计方法和所需审计所需资源的模板。			
31.		**（适用于一、二级）G2.2.3** 应建立审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源的对应关系。	提供审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源的对应关系模板和案例。			
32.		**（适用于一级）G3.2.3 a)** 应利用应用系统工具来建立和维护审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源的对应关系。	提供利用应用系统工具来建立和维护审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源的对应关系的过程证明（可提供相关工具的功能介绍、界面截图等）			
33.		**（适用于一级）G3.2.3b)** 具备为被审计方提供审计范围、审计对象、审计依据要求项、审计程序（方法）、所需资源等对应关系管理工具的能力。				
34.	编制审计实施方案-组建审计组	**G1.2.4 a）** 应考虑审计目标、审计内容、审计范围等组建审计组。	提供审计组管理相关规定。			
35.		**G1.2.4** b） 选择审计组成员应满足通用评价要求的人员能力要求，同时应满足审计和网络安全审计基础流程中的人员能力要求。	提供审计组成员能力评价相关规定。			
36.		**（适用于一、二级）G2.2.4** 应指定审计组	提供包括审计组长、主审和审计组			

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	
		长、主审和审计组成员，并明确分配审计任务。	成员的已组建的审计组案例。			
37.		**（适用于一级） G3.2.4** 对于特定行业领域的网络安全审计，应具备聘请外部行业技术专家作为审计组成员的安排。	提供对于特定行业领域网络安全审计项目，能够聘请外部行业技术专家作为审计组成员的规定。			
38.	**审计取证与评价-审计取证**	**G1.3.1** a) 应选择适当的方法，在现场审计或非现场审计活动中获取审计证据。审计取证的方法可以是访谈、文件和记录调阅、审计项检查表、系统操作验证、审计工具、函证等。	提供审计取证方法，可以是访谈提纲、文件和记录调阅单、审计项检查表、系统操作验证流程、审计工具、函证模板等之一或多种。			
39.		**G1.3.1** b) 在获取审计证据过程中，应选择适当的抽样方式。	提供审计过程中抽样安排的相关规定。			
40.		G1.3.1 c） 应采取必要措施，保证审计证据的相关性、可靠性和充分性。	提供保障审计证据的相关性、可靠性和充分性的相关措施或规定。			
41.		**（适用于一、二级）**G2.3.1 a）应具备至少利用一种网络安全审计工具执行审计取证的能力。	提供至少一种利用网络安全审计工具执行审计取证的记录。			
42.		**（适用于一、二级）**G2.3.1 b）对电子形式存在的审计证据，应做好取证记录，并经被审计方相关人员确认。	提供电子形式的审计证据的取证记录，包括被审计方确认的记录。			
43.		**（适用于一、二级）**G2.3.1 c）应采取必要的措施，保护取证过程中所采集的电子数据的安全。	提供保障电子数据的安全措施或规定。			
44.						

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	
45.		**（适用于一级）G3.3.1** a）应至少具备和使用数据分析类、漏洞和缺陷扫描类、系统配置和运行日志检查类等类型的审计工具的能力。	提供数据分析类、漏洞和缺陷扫描类、系统配置和运行日志检查类等类型审计工具列表，提供使用这些工具开展审计的记录（可以是相关工具的功能介绍、界面截图等）。			
46.		**（适用于一级）G3.3.1** b）利用审计工具取证时，应采取措施确保对审计对象的风险最小化。	提供使用审计工具开展审计的相关操作规定，包括降低风险的措施。			
47.	**审计取证与评价-编制审计工作底稿**	**G1.3.2** a) 应在审计取证完成后，编制审计工作底稿或审计取证单。	提供审计工作底稿或审计取证单模板。			
48.		**G1.3.2** b) 审计工作底稿应内容完整、记录清晰、结论明确，客观地反映项目审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项。				
49.		**G1.3.2** c) 审计工作底稿应经被审计方签字确认。				
50.		**（适用于一、二级）G2.3.2** a） 应建立审计工作底稿的分级复核程序，明确规定各级复核人员的要求和责任。	提供审计工作底稿的分级复核程序，包括各级复核人员的职责描述。			
51.		**（适用于一、二级）G2.3.2** b） 审计工作底稿的内容应包括但不限于被审计部门的名称，审计事项及其期间或者截止日期，审计程序的执行过程及结果记录，审计结论、意见及建议，审计人员姓名和审计日期，复核人员姓名、复核日期和复核	提供审计工作底稿案例，底稿内容包括但不限于被审计部门的名称，审计事项及其期间或者截止日期，审计程序的执行过程及结果记录，审计结论、意见及建议，审计人员姓名和审计日期，复核人员姓名、			

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	
		意见，编号及页次，被审计方意见、附件等。	复核日期和复核意见，编号及页次，被审计方意见、附件等。			
52.		**（适用于一级）G3.3.2** a) 应利用应用系统工具来归档和保管审计工作底稿。	提供利用应用系统工具来归档和保管审计工作底稿的过程证明（可提供相关工具的功能介绍、界面截图等）。			
53.		**（适用于一级）G3.3.2** b) 具备为被审计方提供审计工作底稿管理工具的能力。				
54.	**编制审计工作底稿-审计评价**	G1.3.3 a） 应对审计证据与审计依据的符合性进行评价，以形成审计发现，审计发现应明确审计项符合或不符合审计依据的程度，该程度可以用不同级别来表示。	提供审计发现模板。			
55.		G1.3.2 b) 网络安全审计评价应客观、公正地反映被审计单位信息系统的真实情况。	提供网络安全审计评价原则或相关规定。			
56.		**（适用于一、二级）G2.3.3** 应编制审计发现列表。	提供审计发现列表案例。			
57.		**（适用于一级） G3.3.3** a) 应利用应用系统工具来管理审计发现列表。	提供利用应用系统工具来管理审计发现的过程证明（可提供相关工具的功能介绍、界面截图等）。			
58.		**（适用于一级）G3.3.3** b) 具备为被审计方提供审计发现列表管理工具的能力。				
59.	**审计报告-一般原则**	**G1.4.1** a) 应实事求是地反映被审计事项的事实。	提供网络安全审计报告模板			
60.		**G1.4.1** b) 应要素齐全、格式规范，完整反映审计中发现的重要问题。				
61.		**G1.4.1** c) 充分考虑审计项目的重要性和				

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	
		风险水平，对于重要事项应当重点说明。				
62.		**G1.4.1** d)提出可行的改进建议，以促进被审计方信息系统有效支撑其业务的目标。				
63.		**（适用于一、二级）G2.4.1** 应建立审计报告分级复核程序，明确规定各级复核人员的要求和责任。	提供审计报告分级复核程序（可与**G2.3.2** a)的程序结合），包括各级复核人员的职责描述。			
64.		**（适用于一级）G3.4.1** 应利用应用系统工具来管理审计报告。	提供利用应用系统工具来管理审计报告的过程证明（可提供相关工具的功能介绍、界面截图等）。			
65.	**审计报告-审计报告的内容**	**G1.4.2** a)审计报告应完整、准确地反映审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等。	提供审计报告模板，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等。提供适用的审计报告附件模板。			
66.		**G1.4.2** b)需要时，审计报告可以增加附件。附件内容可包括针对审计过程、审计中发现问题所作出的具体说明，以及被审计单位的反馈意见等内容。				
67.		**（适用于一、二级）G 2.4.2 a）**审计报告中应提出审计发现问题改进建议。	提供审计报告案例。报告中应包括审计发现问题改进建议。			
68.		**（适用于一、二级）G2.4.2** 应建立程序，对已经出具的审计报告可能存在的重要错误或者遗漏及时更正，并将更正后的审计报告提交给原审计报告接收者。	提供审计报告管理规定，包括对审计报告内容更正及重新提交的流程进行规定。			
69.		**（适用于一级）G3.4.2**在审计的任何阶段，如果遇到或发现与审计目标和内容有关的重大问题，如违法违规问题、重大安全	提供审计专报模板或审计专报案例。			

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	
		风险等，应出具审计专报。				
70.	审计报告-交付审计报告	**G1.4.3** a)应建立审计报告的批准和交付程序，保留交付记录。	提供审计报告的批准和交付相关规定。			
71.		**G1.4.3**b) 应在审计委托方或被审计方约定的时间内交付，如延迟交付，应向审计委托方和被审计方说明理由。	提供审计报告的交付管理规定。包括交付时间安排等。			
72.		**（适用于一、二级）G2.4.3** a) 应建立审计报告归档和保管程序。任何组织或者个人查阅和使用归档后的审计报告，必须经审计机构负责人批准，但国家有关部门依法进行查阅的除外。	提供审计报告归档和保管管理相关规定。			
73.		**（适用于一、二级）G2.4.3** b) 审计报告归被审计方所有，被审计方对审计报告的使用、保管等有明确要求的，应遵守其要求。	提供审计报告管理相关规定，包括报告的归属安排等。			
74.		**（适用于一级）G3.4.3** 具备为被审计方提供审计报告管理工具的能力。	提供为被审计方所用的审计报告管理工具。			
75.	跟踪审计-一般原则	**G1.5.1** a)应安排对审计发现问题的整改措施和整改措施的效果进行跟踪审计。	提供审计发现问题的整改措施模板。			
76.		**G1.5.1** b)应与被审计方约定在规定的时间内容实施跟踪审计，一般自审计报告交付起不超过6个月。	提供跟踪审计报告的交付管理规定，包括交付时间安排。			
77.		**（适用于一、二级）G2.5.1** 应编制跟踪审计方案，对后续审计做出安排。	提供跟踪审计方案案例。			

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	
78.	跟踪审计-跟踪审计报告	**G1.5.2** a) 应当根据跟踪审计的实施过程和结果编制跟踪审计报告。	提供跟踪审计报告模板，模板中关键内容需要明确。			
79.		**G1.5.2** b) 跟踪审计报告的管理参照 G1.4 审计报告。	提供跟踪审计报告的管理相关规定。			
80.		**（适用于一、二级）G2.5.2** 跟踪审计报告的管理参照 G2.4 审计报告。				
81.		**（适用于一级）G3.5.2** 跟踪审计报告的管理参照G3.4审计报告。				
82.	审计质量控制-审计质量控制程序	**G1.6.1** a) 应建立审计质量控制程序，以确保遵守审计相关法规和准则，作出准确的审计结论。	提供审计质量控制程序，包括审计质量责任、审计职业道德、审计人力资源、审计业务执行、审计质量监控等。			
83.		**G1.6.1** b) 审计质量控制程序应覆盖审计质量责任、审计职业道德、审计人力资源、审计业务执行、审计质量监控等。				
84.		**（适用于一、二级）G2.6.1 a)** 应建立网络安全审计工作手册，规范网络安全审计全生命周期内的所有活动。	提供适用的网络安全审计工作手册。			
85.		**（适用于一、二级）G2.6.1 b)** 确保审计质量控制程序与网络安全审计工作手册相适应。	提供审计质量控制程序与网络安全审计工作手册，并比较其相关内容的一致性。			
86.		**（适用于一级）**G3.6.1 a) 应监督网络安全审计实施的过程。	提供定期开展网络安全审计质量检查的记录。			
87.		**（适用于一级）**G3.6.1 b) 应定期开展网络安全审计质量检查。				

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	
88.	上一年度提出的观察项整改情况（如有）					
89.						
90.						
91.	上一年度提出的不符合项整改情况（如有）					
92.						
93.						

自评估结论：

经自主评估，本单位的网络安全审计服务满足《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。