信息系统安全运维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 公司安全运维服务规范》、《XX 公司安全运维服务目录》、《XX 公司安全运维问题管理程序》、《XX 项目年度运维总结报告》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《XX 系统巡检记录》、《XX 系统病毒查杀记录》、《XX 项目运维变更单》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 项目安全运维实施方案》第 X 章 项目团队介绍、《XX 项目年度运维服务总结报告》第 X 章 下一年度工作改进计划等，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-安全运维服务流程”、“13-服务级别协议”、“20-安全配置库”、“39-应急响应服务”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	建立信息系统安全运维服务流程。	信息系统安全运维服务流程，流程图中应包括每个阶段对应的职责、输入输出等。			提供《安全运维服务流程》，流程分为四个阶段：准备阶段、实施阶段、监视评审阶段、持续改进阶段，并给出每个阶段的流程图，流程图中给出各个阶段的输入、输出、参与人员角色以及角色所承担的工作职责等内容。 准备阶段： 输入：运维服务合同 输出：客户需求调查报告、客户沟通记录等 职责：需求调研人员通过与客户沟通，确定客户对信息系统运维服务时间的要求，形成需求调查报告得到双方确认等…...
2.		制定信息系统安全运维服务规范并按照规范实施。	信息系统安全运维服务规范并按照规范实施。			提供《安全运维服务规范》，主要包含目的、范围、原则、总体要求、安全运维维护组织、安全运行维护组织职责、安全运行维护工作内容（主要包含安全设备和软件维护、安全

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	
						监控、操作日志、日志审核、故障管理、测试）、安全运行维护计划（包含安全运行维护计划的编制、执行、检查）、安全运行维护报告等章节内容。
3.	准备阶段-需求调研与分析	调研客户信息系统安全现状，采集客户安全服务需求与目标，明确客户对信息系统安全运维服务时间、服务期限、服务内容以及服务方式的需求。	针对客户的调研报告，其中包括对信息系统安全运维服务时间、服务期限、服务内容以及服务方式的需求调研结果。			提供 XX 项目 XXXX（具体文件的名字）文档，文档中对安全运维服务时间、服务期限、服务内容以及服务方式等需求进行了描述，具体信息如下： 1、服务时间：位于 XX 章 XX 节，7*8 小时驻场； 2、服务期限：位于 XX 章 XX 节， 自 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日； 3、服务内容：位于 XX 章 XX 节，内容包含安全策略巡检、日志分析、应急处理、渗透测试等； 4、服务方式：位于 XX 章 XX 节，远程/现场驻守/定期巡检。
4.		进行信息系统运维预算，定义运维服务。	信息系统安全运维预算，其中包括运维服务内容、每项服务的工作量、每项服务的人力资源项目经费等。			提供 XX 项目 XX 文档，文档中 XX 章 XX 节给出运维项目预算表，预算总价：XX 万元，表中包含每个运维服务内容的单价，运

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	
						维内容包含有 XX、XX、XX 等。
5.		与客户进行沟通，达成共识并形成记录 。	与客户沟通形成的记录，内容应有对运维服务项目达成共识的体现。			提供 XX 项目沟通记录（可以是邮件、QQ、微信、会议纪要等）。 例如，邮件的沟通内容为： 沟通时间：XX 年 XX 月 XX 日 沟通对象：XXXX 沟通内容：XXX
6.		**仅二级/一级要求：**分析客户对信息系统安全服务的需求和类型。	对客户进行调查的记录，内容中应有信息系统安全服务的需求和类型，如应用安全：应用系统安全测试、安全监控、安全事件应急等。			提供 XX 项目 XX 文档，文档中 XX 章给出信息系统安全服务的需求和类型，具体包含：应用安全（应用系统安全测试、安全监控、安全事件应急等）、主机安全（漏洞扫描、安全配置核查、补丁更新等）等。
7.		**仅二级/一级要求：**收集与分析信息系统的可用性指标。	所运维信息系统的可用性指标，如整体指标或单系统指标等。			提供 XX 项目 XX 文档，文档中 XX 章 XX 节给出信息系统的可用性指标需求，例如：XX 系统要求可用性不低于 99.99%。

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	
8.		**仅二级/一级要求：**分析以往服务的数据，提取出来未来可自动化的服务。**（监审时适用）**	运维服务报告，其中应对以往安全服务的总结与安全事件的解决效率进行分析，提出未来可自动化的服务。			提供 XX 项目 XX 文档，文档中 XX 章从 XX、XX 等方面对 XX 项目前一年度服务进行总结分析，分析结果显示 XX 服务可以通过 XX 工具实现自动化。
9.		**仅一级要求：**内部团队之间的安全运营级别协议应和与安全运维第三方之间的服务级别设计保持一致。	服务级别协议中，安全运维第三方之间的服务级别设计与内部团队之间的安全运营级别协议应一致。			提供 XX 项目内部团队服务级别协议、以及与第三方签订的 XX 服务级别协议，两份协议中所承诺的 XX、XX 等服务指标目标值一致。
10.		**仅一级要求：**安全组织中要设定安全领导小组。	安全组织架构图，其中应有安全领导小组。			公司已建立包含安全领导小组在内的安全组织架构，安全领导小组包含 XX、XX、XX 等角色，XX 担任 XX 角色。
11.	准备阶段—签订服务协议	与客户签订服务协议，明确范围、目标、时间、内容、金额、质量和输出等。	项目合同及保密协议，合同内容应至少包含服务范围、目标、时间、内容、金额、质量和输出等。			提供 XX 项目合同，合同主要包含以下内容： 合同甲方：XX 公司 合同乙方：XX 合同 XX 条给出服务范围：XX 合同 XX 条给出服务时间：XX 年 XX 月 XX 日-XX 年 XX 月 XX 日 合同 XX 条给出服务内容：XX、XX 合同 XX 条给出合同金额：XX 万 合同 XX 条给出质量要求

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	
						合同 XX 条给出输出成果：XX 总结报告、巡检记录等 合同签订日期：XX 年 XX 月 XX 日 提供 XX 项目保密协议。
12.		明确安全运维的方式，方式包括但不限于：驻场值守方式，定期巡检方式，远程值守方式。	项目合同/协议中应有明确的安全运维模式。			提供 XX 项目合同，合同第 XX 条明确安全运维的方式为：驻场值守方式/定期巡检方式/远程值守方式。
13.		**仅二级/一级要求：**签订服务级别协议。	与客户签订的服务级别协议，协议中应承诺信息系统核心指标，如：可用性、安全事件解决率等。			提供 XX 项目服务级别协议，协议中对 XX、XX、XX 等服务指标的目标值进行了明确，例如：XX 指标要求达到 99%。
14.	方案设计阶段	根据系统安全运维需求，编制安全运维服务方案，明确安全运维服务时间、服务内容、服务方式、服务期限、服务人员、服务交付物、服务质量管理、服务沟通机制、服务风险管理等方面要求。	项目服务方案，内容应包括条款要求。			提供 XX 项目安全运维服务方案，方案 XX 章 XX 节给出安全运维服务时间，XX 章 XX 节给出服务内容，XX 章 XX 节给出服务方式，XX 章 XX 节给出服务期限，XX 章 XX 节给出服务人员，XX 章 XX 节给出服务交付物，XX 章 XX 节给出服务质量管理，XX 章 XX 节给出服务沟通机制，XX 章 XX 节给出服务风险管理。
15.		提供安全设备、业务系统的健康检查服务，并约定服务方式、检查频次和	安全设备、业务系统的健康检查服务记录，应与安全运维服务使用者约定的服务			提供 XX 项目 XX 文档，文档中 XX 章 XX 节对安全设备、业务系统的检查健康服务进

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	
		检查内容。	方式（现场检查，远程检查）、检查频次和检查内容一致，健康检查服务重点关注安全设备、业务系统的可靠性（设备或者系统在一定条件、一定时间下完成一定任务稳定运行的概率）、可用性。			行描述，主要内容为： 检查方式：现场检查/远程检查 检查频次：X 月一次 检查内容：安全设备、业务系统的可靠性（设备或者系统在一定条件、一定时间下完成一定任务稳定运行的概率）、可用性等。
16.		专业人员负责安全管理的接口。	运维项目中由高层指定的、负责安全管理接口的运维管理人员信息。			公司指定 XX 为 XX 项目安全管理接口人。
17.		**仅二级/一级要求：**编制信息系统的可用性计划，监控可用性事件，报告可用性执行，指导可用性的改进。	信息系统可用性计划；信息系统可用性事件记录；信息系统可用性执行报告、改进报告。			提供 XX 项目信息系统可用性计划，计划包含 XX、XX、XX 等章节内容； 提供 XX 项目信息系统可用性事件记录； 提供 XX 项目可用性执行报告； 提供 XX 项目可用性改进报告。
18.		**仅二级/一级要求：**识别与分析信息系统运维过程中的历史数据，提出系统运维的保障策略和解决方案。**（监审时适用**	信息系统运维过程中的分析报告，主要分析项目应有：历史数据清单的分析报告，内容包含运维完成情况、重大事件、重大（失败）变更等；基于以往运维数据分析结果提出的新的运维策略及解决方案。			提供 XX 项目 XX 文档，文档中 XX 章对项目前一年度的运维情况进行分析，分析内容包含 XX、XX、XX 等，针对分析结果中给出的问题，提出了 XX 项目 XX 解决方案，方案主要包含 XX、XX、XX 等章节内容。
19.		**仅二级/一级要求：**编制信息系统的安全基线。	信息系统安全基线。			提供有主机（分为 windows、linux）、数据库、中间件、网络设备、安全设备等安全配

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	
						置基线文档。
20.		**仅二级/一级要求：**建立信息系统安全的配置库。	配置库信息，其中应纳入信息系统安全涉及的配置项，如安全设备的配置项有安全策略、管理员账户、IP 等。			提供 XX 安全配置库（可以利用专门的软件实现，也可以是 excel 等表格形式的配置库），配置库中包含 XX、XX、XX 等资产的 XX、XX、XX 等安全配置项。
21.		**仅一级要求：**建立信息系统应急事件响应机制和恢复保障。	信息系统的应急响应计划和恢复计划。			提供 XX 应急响应计划和 XX 应急恢复计划，应急响应计划包含 XX、XX、XX 等章节内容，应急恢复计划包含 XX、XX、XX 等章节内容。
22.		**仅一级要求：**编制安全运维项目作业指导书。	安全运维作业指导书，例如：配置核查操作手册、常见安全事件处理指南等。			提供 XX 作业指导书。
23.		**仅一级要求：**建立应急响应和灾难恢复机制，形成业务连续性计划。	发布且通过审批的业务连续性计划。			提供 XX 业务连续性计划，计划包含 XX、XX、XX 等内容。
24.		**仅一级要求：**基于漏洞发现与分析进行信息系统漏洞的管理工作。	漏洞管理的方案、流程。			提供 XX 漏洞管理方案，方案包含 XX、XX、XX 等章节内容； 提供 XX 漏洞管理流程，流程主要分为 XX、XX、XX 等 X 个过程或阶段。

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	
25.	运维服务实施	实施初始服务：完成资产识别。	资产识别表，为 IT 资产的标识、分级、保护和软件配置建立基础资料档案；有设备和系统的种类、型号、功能、物理位置、端口对应情况、部署情况等资产详细信息。			提供 XX 资产清单（或者资产表），清单中包含 XX、XX、XX 等资产，记录了每个资产 XX、XX、XX 等详细信息，例如，XX 资产的具体信息如下： 名称：XX 位置：XX 型号：XX 所属系统：XX ……
26.		采集信息系统重要资产的安全配置、流量信息等安全信息。	对组织信息系统的安全配置、流量信息等安全信息进行定期记录。			提供 XX、XX 等资产的安全配置检查记录表； 提供 XX、XX 等资产的流量信息检查记录表。
27.		对安全设备进行日常维护及监控，并记录硬件故障。	安全设备的日常维护记录，包括状态检查、更新、升级、故障检测及排除、对安全设备出现的硬件故障进行统计的记录。			提供 XX 项目 XX、XX 等安全设备的日常维护、状态检查、更新、升级、故障检测及排除记录，内容可以涵盖策略增删改、设备特征库更新、设备升级、设备运行状态检查、常见故障检测等。
28.		收集与分析网络及安全设备、服务器、数据库、中间件、应用系统的日志。	进行安全事件审计，应有对网络及安全设备、服务器、数据库、中间件、应用系统			提供 XX 项目网络设备、安全设备、服务器、数据库、中间件、应用系统日志的审计分析

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	
			日志的保存记录与审计分析报告。			报告。
29.		实施日常巡检服务：对用户的安全设备、网络设备、服务器提供业务操作巡检、状态巡检、安全策略配置巡检服务。	日常巡检记录,主要针对条款要求内容。			提供 XX 项目每日巡检记录（巡检对象至少包含安全设备、网络设备、服务器等，记录中应包含业务操作巡检（例如谁何时登录设备作何操作）、状态巡检（记录设备的 CPU、内容、硬盘等状态信息）、安全策略配置巡检（记录设备的安全策略是否发生变化）等内容）。
30.		实施日常安全运维服务：完成安全设备、网络设备、服务器、应用系统安全事件监控；病毒监测、查杀及网络防病毒维护；漏洞扫描、安全加固、补丁安装；并有相关记录。	日常安全运维服务记录,主要针对条款要求内容。			提供 XX 项目安全设备、网络设备、服务器、应用系统安全事件监控记录（可以通过查看安全设备的相关攻击或者阻断日志信息实现安全事件的监控，也可以通过专门的安全事件监控系统实现）； 提供 XX 项目病毒查杀、监测记录； 提供 XX 项目的漏洞扫描记录，提供漏洞扫描结果； 提供 XX 项目的安全加固记录，提供具体的加固对象及加固内容； 提供 XX 项目的补丁安装记录，记录具体安

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	
						装补丁的信息，例如补丁名称、安装时间、安装人等。
31.		对信息安全事件进行统计与分析。	信息安全事件的统计表，分析报告。			提供 XX 项目信息安全事件统计表，记录安全事件发生的次数，并提供事件发生的原因及分析记录。
32.		实施健康检查服务：完成安全设备、业务系统的健康检查服务。	安全设备、业务系统的健康检查服务记录，主要关注可靠性、可用性、持续性等。			提供 XX 项目健康检查记录，检查对象包含 XX、XX、XX 等，检查内容包含 XX、XX、XX 等。
33.		**仅二级/一级要求：**收集与建立配置管理数据库，确保配置项目的机密性、完整性、可用性（专职管理）。	配置数据库，应能初步收集资产与配置项，并确保配置项目的机密性、完整性、可用性（专职管理），如安全设备的配置项有安全策略、管理员账户、IP 等。			提供 XX 配置数据库，配置数据库中包含 XX、XX 等资产及其关键配置项，配置项包含 XX、XX、XX、XX 等。
34.		**仅二级/一级要求：**实施安全设备、网络设备、中间件、数据库、服务器等资产的安全配置管理，定期对配置项进行更新和维护。	配置项的更新和维护记录。			提供 XX 项目 XX、XX 设备配置项更新与维护记录，记录中包含更新或者维护的时间、内容、人员等信息。
35.		**仅二级/一级要求：**根据制定的安全配置基线，定期进行安全配置核查工作。	安全配置核查记录。			提供 XX 项目安全配置核查记录，核查对象包含 XX、XX、XX 等。
36.		**仅二级/一级要求：**实施运维监控与分析并形成记录。	对各类安全事件的集中管理和分析记录。			提供 XX 项目安全事件的监控与分析记录，记录包含 XX、XX、XX 等主要内容。

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	
37.		**仅一级要求：**实施安全培训服务：完成安全意识、基本安全技术的培训服务。	安全培训服务记录。			提供 XX 项目安全培训服务记录，培训内容涉及 XX、XX 等方面。
38.		**仅一级要求：**实施安全通告及漏洞分析服务：完成业界动态的通告、收集国家安全政策及法律法规、漏洞通告、病毒通告、厂商安全通告及其他安全通告。	通告与漏洞分析记录，内容为业界动态的通告、收集国家安全政策及法律法规、漏洞通告、病毒通告、厂商安全通告及其他安全通告，以及基于通告进行的分析。			提供 XX 项目安全漏洞通告记录，通告内容涉及 XX、XX、XX 等安全漏洞； 提供 XX、XX、XX 等安全漏洞分析记录。
39.		**仅一级要求：**实施应急响应服务：完成应急响应预案制定，对应急事件及时响应，并对应急预案进行演练，形成相关记录。	应急响应记录； 应急响应预案，应急演练的记录。			提供 XX 项目应急响应记录，记录包含 XX、XX 等内容； 提供 XX 项目应急响应预案，预案包含 XX、XX 等内容； 提供 XX 项目应急演练记录，记录包含 XX、XX 等内容。
40.		**仅一级要求：**依据运维变更管理程序，对运维实施过程中方案、资源变更进行有效控制，完整记录变更过程。	运维过程中的变更记录。			提供《运维变更管理程序》，提供 XX 项目变更记录。
41.		**仅一级要求：**制定运维应急处置方案和恢复策略，对运维过程中的应急事件及时进行响应。	应急处置方案和恢复策略；运维过程中的响应时间应达到方案要求。			提供 XX 项目应急处置方案和恢复策略，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	
42.		**仅一级要求：**依据风险评估方案与计划实施信息系统风险评估；依据渗透测试方案与计划实施信息系统渗透测试。	风险评估记录与报告； 渗透测试报告。			提供 XX 项目的风险评估方案、风险评估记录、风险评估报告。 提供 XX 项目的渗透测试报告。
43.		**仅一级要求：**依据漏洞管理方案实施信息系统漏洞管理工作。	运维服务过程中漏洞的发现、分析、验证、跟踪、修复等过程记录。			提供 XX 项目的漏洞发现、分析、验证、修复记录，漏洞包含 XX、XX、XX 等。
44.	运维服务报告	向客户提交服务报告，定期收集与报告安全运维实施情况。	安全运维的定期服务报告,服务报告应对一段时间内运维服务实现情况进行统计与分析。			提供 XX 项目的服务报告（包含周报、月报、季报等）。
45.		汇总整理全年服务记录，形成年终安全运维服务总结报告。	年终安全运维总结报告，对全年的服务情况进行总结与分析。			提供 XX 项目的年度总结报告，报告包含 XX、XX、XX 等章节内容。
46.		根据合同约定，配合组织项目验收，出具项目验收报告。	项目验收报告。			提供 XX 项目验收报告，验收时间：XX 年 XX 月 XX 日。
47.		**仅二级/一级要求：**应定期收集与分析安全运维的关键指标数据，数据包括但不限于：异常报告及时率、异常漏报率、故障隐患发现率、异常主动发现率、问题解决率、漏洞扫描覆盖率、加固设备覆盖率、安全补丁安装及时率、安全事件次数。（参照服务合同）	运维服务报告，其中的统计分析数据应包括：异常报告及时率、异常漏报率、故障隐患发现率、异常主动发现率、问题解决率、漏洞扫描覆盖率、加固设备覆盖率、安全补丁安装及时率、安全事件次数。			提供 XX 项目运维数据的收集与分析报告，报告中对 XX、XX、XX 等指标的完成情况进行了统计分析。

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	
48.		**仅二级/一级要求：**建立客户满意度调查机制。	客户满意度调查的方式、方法、分析方法等；满意度调查的实施情况与分析情况。			提供 XX 项目的满意度调查表，调查内容包含 XX、XX、XX 等。
49.		**仅一级要求：**对客户满意度进行趋势分析。	客户满意度调查报告与趋势分析报告。			提供 XX 项目满意度调查分析报告，包含 XX、XX、XX 等内容。
50.		**仅一级要求：**对客户系统的安全态势做出分析，并给出安全建议。	对客户系统的安全态势分析报告，报告中需给出针对性的安全加固处理建议。			提供 XX 项目安全态势分析报告，报告包含 XX、XX、XX 等内容。
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，本单位的信息系统安全运维服务满足《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。