信息系统安全运维服务资质认证自评估表

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。			
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。			
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。			
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。			
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。			

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	
6.		**仅二级/一级要求：**分析客户对信息系统安全运维服务的需求和类型。	对客户进行调查的记录，内容中应有信息系统安全运维服务的需求和类型，如应用安全：应用系统安全测试、安全监控、安全事件应急等。			
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。			
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进行总结，对安全事件的解决效率进行分析，适宜时提出未来可自动化的服务。			
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。			
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。			
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。			
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。			

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	
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。			
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。			
15.		在安全运维服务方案中明确健康检查服务的服务方式、检查频次和检查内容。	项目服务方案对健康检查服务的服务方式、检查频次和检查内容进行明确。			
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。			
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。			
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**	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			

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	
		时适用	（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。			
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。			
20.		**仅二级要求：**建立信息系统安全配置库。	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。			
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。			
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。			
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。			
24.		**仅一级要求：**在安全运维服务方案中明确漏洞管理的工作流程。	漏洞管理的方案、流程。			
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			

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	
			息。			
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。			
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。			
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、应用系统日志的保存记录与审计分析报告。			
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。			
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。			
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。			

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	
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。			
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。			
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。			
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。			
36.		**仅二级/一级要求：**实施运维监控与分析并形成记录。	完成对各类安全事件的集中管理和分析，以数据来分析各个指标的趋势，形成相关记录。			
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。			
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、	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			

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	
		病毒通告、厂商安全通告及其他安全通告。	安全通告，以及基于通告进行的分析。			
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。			
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。			
41.						
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。			
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。			
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。			
45.		汇总整理全年服务记录，形成年终安	年终安全运维总结报告，对全年的服务情			

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	
		全运维服务总结报告。	况进行总结与分析。			
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。			
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。			
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。			
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。			
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。			
51.	**上一年度提出的观察项整改情况（如有）**					
52.						

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	
53.						
54.	上一年度提出的不符合项整改情况（如有）					
55.						
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。