# 信息系统安全运维服务资质认证自评估表（试用版）

|  |  |  |  |
| --- | --- | --- | --- |
| **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** |
|  | 准备阶段—需求调研与分析 | 采集客户对信息系统运维服务时间的需求。 | 运维前的客户需求调查报告，可结合结合业务部门，公司高层的战略规划，内容必须有服务时间要求。 |  |  |  |
|  | 进行信息系统运维预算，定义运维服务。 | 运维前的信息系统运维预算表,内容应包括工作量、人力资源项目经费、项目节点等。 |  |  |  |
|  | 与客户进行沟通，达成共识并形成记录 。 | 运维前与客户沟通的记录，应有沟通结果双方达成共识的体现。 |  |  |  |
|  | **仅二级要求：**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。 | 信息系统运维过程中的历史数据清单；历史数据清单的分析报告，内容包含指标完成情况、违例操作、重大事件、重大（失败）变更等。根据报告的分析制定的运维策略，及实施方案； |  |  |  |
| **仅二级要求：**分析客户对信息系统安全服务的需求和类型。 | 客户需求调查报告，包含信息系统安全服务的需求和类型； |  |  |  |
|  | **仅二级要求：**收集与分析信息系统的可用性指标，明确可用性指标的类型。 | 信息系统的可用性指标清单，如整体指标或单系统指标等； |  |  |  |
|  | **仅二级要求：**分析以往服务的数据，提取出来未来可自动化的服务。 | 以往提供服务的解决方案，对生产的影响的分析报告；根据以往安全事件的解决效率进行分析，适宜时提出来未来可自动化的服务。 |  |  |  |
|  | **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的服务级别设计保持一致。 | 服务级别设计、安全运营级别协议，两者应保持一致。 |  |  |  |
|  | **仅一级要求：**安全组织中要设定安全领导小组；在采用外包模式的情况下，执行组还应包含安全运维服务供应商参与运维的人员。 | 安全组织架构图及相关运维人员清单，其中应有安全领导小组；外包模式的执行组中应有第三方参与运维的人员。 |  |  |  |
|  | **仅一级要求：**采用基于PDCA的管理模型，从策划，实施，监视与评审和持续改进进行体系化的信息系统安全运维服务。 | 信息系统安全运维服务有策划，实施，监视与评审和持续改进流程。 |  |  |  |
|  | **仅一级要求：**建立安全运维可视化视图。基于信息系统安全的生命周期，建立信息系统安全运维的整体策略。基于客户、业务的价值体现，形成安全运维的整体视图。 | 安全运维项目施工手册和作业指导书；新建系统，建设实施过程应重点关注信息系统的功能、性能和安全性等方面要求，应保留与客户的需求分析记录；系统改造中考虑造前技术测试验证及在实施失败后的回退措施；测试验证中对旧系统的兼容问题，包括网络兼容、系统兼容、应用兼容等，有验证报告。 |  |  |  |
|  | 准备阶段—运维服务设计 | 制定安全运维服务目录，目录内容包括但不限于：初始服务、安全设备运维、日常巡检服务、健康检查、安全事件审计。 | 安全运维服务目录，内容包含条款要求。 |  |  |  |
|  | 信息系统相关的IT资产进行识别。 | IT资产识别清单，内容有IT资产识别的标识、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。 |  |  |  |
|  | 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，状态检查，定期查杀，故障处理、保养、更新、升级、故障检测及排除，并对安全设备出现的硬件故障进行统计的记录。 |  |  |  |
|  | 提供安全设备、业务系统的健康检查服务，并约定服务方式、检查频次和检查内容。 | 有安全运维服务使用者约定的服务方式（现场检查，远程检查）、检查频次和检查的文件记录。 |  |  |  |
|  | 采集系统配置、流量信息、系统状态等安全信息。 | 安全设备、业务系统的健康检查服务，应与安全运维服务使用者约定的服务方式（现场检查，远程检查）、检查频次和检查的文件的记录。 |  |  |  |
|  | 收集与分析网络及安全设备、服务器、操作系统、网络应用的日志。 | 有对网络及安全设备日志，服务器、操作系统等日志，网络应用日志的记录与分析报告。 |  |  |  |
|  | **仅二级要求：**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；信息系统的可用性事件、计划、报告；安全运维角色清单。 |  |  |  |
|  | **仅二级要求：**编写安全运维服务目录，目录内容包括但不限于：运维监控与分析、终端安全监控、等级保护合规性运维。 | 安全运维服务目录，内容应包含有条款的要求。 |  |  |  |
|  | **仅二级要求：**建立信息系统安全运维的问题管理程序。 | 信息系统问题管理程序，已审批并发布。 |  |  |  |
|  | **仅二级要求：**建立知识管理程序及初步形成知识库。 | 知识管理程序，已审批并发布。 |  |  |  |
|  | **仅二级要求：**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。 | 信息系统的可用性事件、计划、报告。 |  |  |  |
|  | **仅二级要求：**形成信息安全管理的组织架构，组织结构的构成要素与安全运维活动角色相对应。 | 信息安全管理的组织架构表，安全运维角色清单，应与组织的构成要素对应。 |  |  |  |
|  | **仅一级要求：**编制安全运维项目作业指导书。 | 安全运维项目中各模块作业指导书。 |  |  |  |
|  | **仅一级要求：**建设实施过程中应关注信息系统的功能、性能和安全性方面要求。改造过程中应制定测试计划及回退措施。 | 有改造过程中的信息系统的测试计划；有信息系统的基线、回退的措施文件。 |  |  |  |
|  | **仅一级要求：**编写安全运维服务目录，目录内容包括但不限于：安全通告及漏洞分析、应急响应服务。 | 安全运维服务目录，内容有条款要求的服务。 |  |  |  |
|  | 准备阶段—运维服务导入 | 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。 | 完整的配置数据库，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。 |  |  |  |
|  | 专业人员负责安全管理的接口。 | 完整的配置数据库，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。 |  |  |  |
|  | 建立服务目录。 | 安全运维服务目录。 |  |  |  |
|  | 建立事件响应和解决的机制,有基本的安全运维报告模式。 | 安全事件处理与应急响应流程，安全事件处理与上报流程。 |  |  |  |
|  | **仅二级要求：**采用流程化管理方法，基于安全事件处理流程、安全培训服务流程、渗透测试流程进行标准化的信息系统安全运维工作。 | 渗透测试的计划和记录；建立安全事件处理流程，安全培训服务流程，渗透测试的流程。 |  |  |  |
|  | **仅一级要求：**基于渗透测试流程管理进行标准化的信息系统安全运维工作。 | 运维过程中的渗透测试的计划和记录。 |  |  |  |
|  | **仅一级要求：**编制信息安全产品和工具定制开发计划。 | 信息安全产品和工具定制开发计划，内容可以应客户要求或组织自身的能力。 |  |  |  |
|  | 准备阶段—服务协议的特殊要求 | 明确安全事件处理与应急响应流程，流程包括但不限于：安全事件的分类、安全事件上报流程、安全事件处理流程、安全事件的事后处理。 | 建立安全事件处理流程，应急响应流程，内容应包括条款要求； |  |  |  |
|  | 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。 | 服务级别协议协议，其中内容包括运维的方式。 |  |  |  |
|  | **仅二级要求：**签订服务级别协议,建立信息系统应急事件响应机制和恢复保障。 | 服务级别协议，内容包括承诺信息系统核心指标；应急响应计划、系统恢复计划。 |  |  |  |
|  | **仅二级要求：**建立问题管理程序。 | 信息系统的问题管理程序，已审批并发布。 |  |  |  |
|  | **仅二级要求：**建立信息系统安全的配置库及关联关系信息。 | 配置库，系统安全配置项之间有关联信息。 |  |  |  |
|  | **仅一级要求：**建立信息系统安全运维服务级别管理程序，签订服务级别协议。 | 有已通过审核并发布的信息系统安全运维服务级别管理程序；查看客户有服务级别协议。 |  |  |  |
|  | **仅一级要求：**建立信息系统应急事件响应机制和恢复保障。 | 应急响应计划、系统恢复计划的演练记录； |  |  |  |
|  | **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； |  |  |  |
|  | **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。 |  |  |  |
|  | 服务实施阶段 | 实施初始服务：完成资产识别，定期配置项的更新和维护，实施相关运维流程。 | 资产识别表，对配置项的更新和维护记录，实施相关运维流程的记录。  |  |  |  |
|  | 实施安全设备运维服务：完成日常维护，状态检查，定期查杀，故障处理、保养、更新、升级、故障检测及排除，并对安全设备出现的硬件故障进行统计记录。 | 日常维护，巡检、状态检查，定期查杀，故障处理、保养、更新、升级、故障检测及排除的记录； |  |  |  |
|  | 实施日常巡检服务：完成安全设备监控；病毒监测、查杀及网络防病毒维护，并有相关记录。 | 信息安全事件审计报告，如网络及安全设备日志、服务器、操作系统、网络应用的日志； |  |  |  |
|  | 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，主要工作针对于设备的可用性、持续性，并提供相应服务记录。 |  |  |  |
|  | 实施安全事件审计服务：完成网络及安全设备日志、服务器、操作系统、网络应用的日志、并且进行记录。 | 实施安全事件审计服务，内容包含条款中的要求。 |  |  |  |
|  | 组建运维服务台职能，培养服务台人员的专业能力。 | 建立服务台；提供服务台人员的培训记录。 |  |  |  |
|  | 建立事件管理程序和信息安全服务请求管理程序。 | 事件管理程序，已审批并发布；服务请求管理程序，已审批并发布。 |  |  |  |
|  | **仅二级要求：**实施运维监控与分析并形成记录。 | 运维监控分析报告，内容以数据来分析各个指标的趋势。 |  |  |  |
|  | **仅二级要求：**进行等级保护合规性运维。 | 针对信息系统安全建立保护等级；对信息系统分级的标准； |  |  |  |
|  | **仅二级要求：**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，并生成分析报告。 |  |  |  |
|  | **仅二级要求：**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，并对应急进行演练，形成相关记录 | 通告与漏洞分析记录；应急响应服预案，应急演练的记录；变更管理程序，已审批并发布；运维过程中的变更记录单。 |  |  |  |
|  | **仅一级要求：**建立运维变更管理程序，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。 | 针对运维有审批并发布的变更管理程序；运维过程中的变更应有响应的变更记录。 |  |  |  |
| **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。 | 有已审批并发布的应急处置方案和恢复策略；运维过程中的响应时间是否达到方案要求。 |  |  |  |
|  | 监视评审阶段 | 应定期收集与分析安全运维报告的数据，包括但不限于：异常报告及时率、异常漏报率、维护作业计划的及时完成率、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。 | 运维数据收集记录，内容应包含条款中的要求。  |  |  |  |
|  | 对运维实现情况进行监视测量，未能实现的目标应采取纠正预防措施。 | 安全运维实现情况监视测量清单，如客户满意度、投诉建议、KPI等；纠正预防措施记录单。 |  |  |  |
|  | 建立与分析客户满意度调查。 | 客户满意度调查报告，内容应包括对满意度分析。 |  |  |  |
|  | **仅二级要求：**按照计划的时间间隔执行内部审核，应至少满足： 既定标准的要求、满足安全运维服务需求和客户所提出的SMS要求、 有效被实施和维护。 | 内部审核的响应文件与记录；管理评审的响应文件与记录，内容应包含服务和流程的执行情况和符合性； |  |  |  |
|  | **仅二级要求：**定期回顾安全运维服务，确保其持续适用和有效。管理评审的输入至少包括：客户反馈、服务和流程的执行情况和符合性、当前和预测资源水平、纠正措施的进展情况、可能影响安全运维服务的变更、改进的机会。 | 当前和预测资源水平；纠正措施的进展情况；可能影响安全运维服务的变更；改进的机会，如指标为满足、运维中存在的问题、服务提升点等。 |  |  |  |
|  | **仅一级要求：**形成体系化的审核机制及企业文化。 | 内部审核机制形成体系，表现形式如：体系文件、PDCA流程、第三方认证等；建立服务监视管理流程 |  |  |  |
|  | **仅一级要求：**体系化的服务监视管理，形成审核机制。 |  |  |  |
|  | **仅一级要求：**定期评审客户对安全运维服务的满意度。 | 客户满意度调查表，包括：定期评审、主动回访等。 |  |  |  |
|  | 安全运维运—维持续改进 | 应在运维过程和监视过程中识别改进项目，制定持续改进计划，计划应包括对改进机会的评估标准。 | 安全运维持续改进计划；查看改进计划的评估标准。包括：识别过程、记录过程、是否有批准过程、评估、测量和适合的报告机制。 |  |  |  |
|  | 应有文件化的程序用以识别、记录、批准、评估、测量和报告改进措施。 |  |  |  |
|  | 应采取预防措施，以消除潜在的不符合项的原因，以防止其发生。 | 安全运维预防措施文件，及其有效性验证的记录。 |  |  |  |
|  | **仅二级要求：**改进机会应划分优先级，策划被批准的改进机会。 | 改进机会分析报告，及其批准证据；优先级排序的方式不限，但应有合理性。 |  |  |  |
|  | **仅二级要求：**改进活动应进行管理，至少包括： 设定改进目标、确保批准的改进活动被实施、报告被实施的改进计划。 | 改进活动的计划、实施、有效性测量记录；内容包括设定改进目标、确保批准的改进活动被实施、报告被实施的改进计划。 |  |  |  |
|  | **仅一级要求：**持续服务改进，形成持续服务改进文化和意识。 | 有服务改进的意识以培训，宣贯的方式传达到员工，有相应的记录。 |  |  |  |
|  | **仅一级要求：**基于运维服务的缺陷，提出改进策略和方案。 | 对运维的重大事件、失败变更、服务不达标等不良情况进行分析，提出改进计划。 |  |  |  |
|  | **仅一级要求：**分析运维服务的数据并进行服务预测。 | 对运维的数据如日志、变更、事件、请求、问题进行汇总分析，预测服务的导向。 |  |  |  |
|  | **上一年度提出的观察项跟踪验证情况（如有）** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | **上一年度提出的不符合项跟踪验证情况（如有）** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**自评估结论：**

经自主评估，本单位的信息系统安全运维服务资质满足ISCCC-SV-001:2015《信息安全服务资质认证实施规则》 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。**

**单位法人签字（公章）：**

**时间： 年 月 日**