方案评审记录单

记录编号：$项目编号$—VG9—01

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **基本信息** | **项目名称** | | $项目名称$ | | **项目类型** | G | |
| **评审类型** | | ☑ 方案评审 | | | | |
| **评审方式** | | ☑ 会签评审 □ 会议评审（会议纪要编号： ） | | | | |
| **评审时间** | | $方案编制末日$ | | | | |
| **评审材料** | | $项目编号$\_GF01\_项目方案\_$项目名称$  LD18-11 信息系统基本情况调查表-$项目名称$  LD18-31等级保护测评项目计划书-$项目名称$ | | | | |
| **评审记录** | | | | | | | |
| **评审项** | | **评审内容** | | **结果记录** | | | **是否符合** |
| **规范性** | | 1. 模板——使用最新模板，对未描述的内容不应删除，对不适用的内容，应给出说明 2. 标识——每项内容都有相应的标识 3. 图表——图表的标题、图表的跨页、颜色配比不影响打印 4. 段落文字——段落设定与模板一致 5. 文字——不应出现错字、别字或影响用户识别的字体，一般都应以中文给出（中英文对照） | | * 《$项目编号$\_GF01\_项目方案\_$项目名称$》使用了最新A2.5模板，符合要求；没有删除章节，对不适用的内容进行了说明； * 对每项内容都进行了标识，有完整的目录，并对目录进行了更新； * 图表完整，排版正确； * 段落设定和模板一致； * 未出现错字、别字或影响用户识别的字体。 | | | **符合** |
| **一致性** | | 1. 文内一致——文档内描述应保持一致的、不冲突的 2. 图表一致——文字描述和图表一致 3. 文档间一致——文档间内容一致，与调查表和项目计划书一致 | | * 《$项目编号$\_GF01\_项目方案\_$项目名称$》文档内容前后一致，未见矛盾之处； * 文字描述与图表一致，采用了正确的网络拓扑图； * 文档与系统调查表、项目计划书等保持一致，设备名字和其他信息与调查表保持一致。 | | | **符合** |
| **总体架构** | | 1. 系统——对项目概况和被测系统进行描述 2. 职责——测评双方人员职责是否明确，分工是否合理 3. 方法——测评方法是否明确、有效和符合程度 4. 环境——被测系统的机房、拓扑图、应用、数据的描述 | | * 《$项目编号$\_GF01\_项目方案\_$项目名称$》描述了被测系统的定级情况，为$等级$。 * 方案描述了测评双方人员及职责，测评内容与实施对双方工作进行了说明，分工合理； * 测评方法包括访谈、检查、测试，能满足系统的测评需求； * 网络结构和系统构成描述清晰，符合测评的要求。 | | | **符合** |
| **测试对象选择** | | 1. 对象——测评对象的选择是否明确、合适、具有典型性 2. 强度——测评强度是否达到测评等级要求 | | * 测评对象选择符合选择原则要求，针对服务器，挑选了安装应用和数据库的服务器； * 选择的测评对象符合$等级$测评的强度要求。 | | | **符合** |
| **测评资源** | | 1. 工具——测试工具与手段满足测评要求 2. 指导书——作业指导书编制完整，编制缺少作业指导书 3. 测试资源——现场测试的计划与资源安排的合理、可行，不会互相产生影响 | | * 主要测评工具包$设备名称$，结合测评方法，能满足$等级$的测评要求。 * 各方面的作业指导书都已经编写完成； * 现场测评时间安排合理可行，且不会互相产生影响。 | | | **符合** |
| **接入点选择** | | 1. 现场测评——内容是否涵盖现场测评、扫描和渗透测试 2. 接入点——测试工具的测试路径和接入点，明确扫描对象和目的 3. 模拟测试——是否在仿真环境中进行过模拟测试，不会对系统造成影响 | | * 现场测评、扫描符合测评要求； * 扫描与渗透的风险描述清晰，包括测试接入点和测试对象等； * 测试从正式环境/仿真环境中进行扫描。 | | | **符合** |
| **测评指标** | | 1. 指标——根据系统分级要求对指标进行确定 2. 不适用安全子类——是否列出了不适用安全子类及理由 3. 测评依据——对用户要求的特定标准或行业规范进行补充 | | * 系统定级为$等级$，章节3.1测评指标共$测评指标项数$项，符合定级要求。 * 根据系统的实际情况，描述了不适用的对象； * 测评依据包括GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》、GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》、JR/T 0071.2-2020：《金融行业网络安全等级保护实施指引 第 2 部分：基本要求》、JR/T 0072—2020：《金融行业网络安全等级保护测评指南》、GB/T 17859—1999《计算机信息系统 安全保护等级划分准则》、GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》、GB/T 20984-2007《信息安全技术 信息安全风险评估规范》等，涵盖了所需的标准及行业规范。 | | | **符合** |
| **风险** | | 1. 现场测评——描述测评过程中可能存在的风险，包括测评前，需要用户授权现场测评 2. 渗透测试——对渗透等现场测试活动的风险进行分析，并和客户及时、充分沟通，必要时建议用户进行备份、恢复 | | * 本文描述了现场测评的风险，风险描述完整且符合实际情况； * 对于渗透测试的风险进行了分析，并与客户及时沟通，并建议客户进行备份。 | | | **符合** |
| **其它** | |  | |  | | |  |
| **评审**  **结论** | | ☑ 评审通过  □ 需要进行整改并复核后评审通过  □ 修改后重新评审  **方案编制合理，资源可以满足需求。**  评审人：  日期：$方案编制末日$ | | | | | |
| **整改情况** | | 项目负责人： 完成日期： | | | | | |
| **备注：** | | | | | | | |

注：记录编号应填写为：#（项目编号）—VG9—nn（顺序号）