信息系统安全等级测评报告质量检查单

记录编号：$项目编号$-VG7-01

|  | 修改项 | 修改内容 | 确认 |
| --- | --- | --- | --- |
|  | 全文 | 删除红色“填写说明” | √ |
|  | 报告封面 | 删除“项目编号：P20XXXXXXX” | √ |
| “系统名称”—“报告时间”的内容替换为附录一的表格 | √ |
| 报告编号：第三段为年份，与“报告日期”的年份一致 | √ |
| 核对报告封面的内容，“系统名称”、“委托单位”与备案证明、“系统安全等级保护备案表”、测评管理平台保持一致 | √ |
|  | 网络安全等级测评基本信息表 | 编制人、审核人、批准人：删除“（签字）” | √ |
| 编制人：项目经理电子签章 | √ |
| 完善“编制日期”、“审核日期”、“批准日期”，三个日期可为同一天  日期格式（除封面“报告时间”）：20XX年XX月XX日  编制日期=“1.3测评过程”中 分析与报告编制过程的截止日期  批准日期>=审核日期  报告日期=批准日期= “声明”页中的日期 | √ |
| 机构代码：310072  “测评单位-联系人-所属部门”填写“网络安全技术研究所” | √ |
|  | 声明 | 本报告记录号：P202YMMNNN-GB01  要求：仿宋\_GB2312，四号，空两格另起一段 | √ |
|  | 等级测评结论-被测对象描述 | 包括**系统主要功能、网络边界和网络区域等，**样例见附录二 | √ |
| **描述通顺、有条理** | √ |
|  | 等级测评结论-测评工作描述 | 采用测评能手导出模板，包括**测评时间、测评范围、测评过程**等，样例见附录二。 | √ |
| 删除测评工作描述中“具体如图 1.1 所示。” | √ |
| **描述通顺、有条理** | √ |
|  | 等级测评结论扩展表（云计算安全） | 在没有更明确的要求前，对于云租户测评时，报告中“等级测评结论扩展表（云计算安全）”的“云计算服务安全能力评价”可暂不填写，样例见附录三。  若填写“云计算服务安全能力评价”，则应对所提供功能进行描述，而非仅描述对应要求是否“符合” | √ |
| 若为云租户，该表中信息均为其所在云平台相关信息，“运维所在地”、“等级测评结论”、“综合得分”均为云平台测评相关信息，由云平台提供 | √ |
| 测评对象若有多个角色，则报告中应按照不同角色填写相应的”等级测评结论扩展表（云计算安全） | √ |
| 关于云扩展要求在“私有”环境是否适用的问题，建议根据环境中是否有“租户按需自助”来进行判断  如用户方（私有云）坚持要使用云扩展，也可使用云扩展进行测评，但相应发现的问题用户方也需要接受 | √ |
| 若被测对象未使用云计算技术，则删除 | √ |
|  | 等级测评结论扩展表（大数据安全） | 删除 | √ |
|  | 总体评价 | 以测评能手导出模板为准，核对总体评价中的“不适用数” | √ |
| **三防措施**每个单独一段描述，见附录四 | √ |
| **描述通顺、有条理** | √ |
|  | 1.1测评目的 | 以测评能手导出为准，不采用原实验室模板 | √ |
|  | 1.2测评依据 | 选择了符合要求的**基本要求、行业标准和扩展标准** | √ |
| 在最后增加标准：   * GB/T 20984-2007：《信息安全技术 信息安全风险评估规范》   格式同其他标准 | √ |
|  | 1.3 测评过程 | 原则上测评准备过程、方案编制过程不少于2天，现场实施过程、分析与报告编制过程不少于3天；  现场实施过程包括初测和复测阶段  时间前后无矛盾或不一致 | √ |
| 包括项目启动会议、末次会议  项目启动会议：方案编制过程第一天（与方案评审不同时召开）或现场实施第一天（与方案评审同时召开）  方案评审日期：方案编制最后一天或现场实施第一天  末次会议：现场测评结束日期 | √ |
| **测评过程与平台流转一致** | √ |
|  | 1.4 报告分发范围 | 修改为“等级测评报告正本一式三份，其中AAAAA一份，上海市公安局一份，上海计算机软件技术开发中心一份。” | √ |
|  | 2.1.2 业务和采用的技术 | 系统主要功能描述、截图，业务和技术描述合理 | √ |
|  | 2.1.3 网络结构 | 网络拓扑图**绘制清晰**（能体现网络结构、设备能唯一识别）、架构描述（区域划分、区域间隔离和防护措施），能体现数据流向 | √ |
|  | 2.2 测评指标  2.2.1 安全通用要求指标 2.2.2 安全扩展要求指标 | 整个“安全层面”不适用时应删除，同步修改总数 | √ |
|  | 2.2.2 安全扩展要求指标 | 若无安全扩展要求指标，替换这一段为“本次测评未涉及安全扩展要求指标。” | √ |
|  | 2.2.3 其他安全要求指标 | 若无其他安全要求指标（如邮件专项），替换这一段为“本次测评未涉及其他安全要求指标。” | √ |
|  | 2.2.4 不适用指标 | 指标不适用的理由充分合理 | √ |
| 整个测评项不适用，则列入不适用指标，仅单个测评对象不适用而其他测评对象适用，应删除不适用指标中相关行 | √ |
| 核对“表中不适用指标数量” | √ |
|  | 2.3.1 测评对象选择方法 | 采用实验室模板 | √ |
|  | 2.3.2 测评对象选择结果 | 抽样至少需要覆盖到所有设备/操作系统/数据库的类型、重要设备全选、覆盖所有网络边界、网络区域边界，常见测评对象示例见“附录五” | √ |
|  | 3.X.1 已有安全控制措施汇总分析 | 增加符合情况的描述  测评内容完整，没有应测未测的情况，结果分析合理 | √ |
|  | 3.X.2 主要安全问题汇总分析 | 核对“问题描述”和“涉及测评对象”的对应关系，例：  问题描述：**应用系统**未采用密码技术进行存储完整性验证  涉及测评对象：**核心交换机、防火墙……** | √ |
| 若安全层面具有低风险安全问题而此处测评能手导出内容为“无”，则增加低风险安全问题的相关描述 | √ |
|  | 3.4.4 其他系统和设备 | 修改为“本次测评未涉及其他系统和设备。” | √ |
|  | 3.11 其他安全要求指标 | 若无其他安全要求指标（如邮件专项），替换这一段为“本次测评未涉及其他安全要求指标。 | √ |
|  | 3.12 验证测试 | 测评工具和接入点选择合理，满足测评强度和内部规范要求  原则：**扫描需在不经过安全防护策略的情况下进行**  云平台：应用扫描，需白名单策略，也可在测试环境进行（用户保证应用一致）  非云平台外网应用：在内网扫描主机、应用（B/S架构），扫描发现问题在外网验证  内网应用：扫描主机、应用（B/S架构） | √ |
| 将图3.1调整到该节文字之后 | √ |
| 删除“注：若由于用户原因无法开展验证测试，应将用户签章的“自愿放弃验证测试声明”作为报告附件。”这一段 | √ |
| “本次测评采用的工具有：”根据实际测评情况修改表格内容，使用实验室有授权的工具（绿盟、安恒、webray、nessus）  注意扫描工具版本、特征库的更新 | √ |
|  | 4.2 区域间/层面间安全测评 | 区域间、层面间安全测评的相关描述均在本段中描述 | √ |
|  | 4.3 整体测评结果汇总 | 原则上需根据情况进行整体测评  若整体测评内容为空，修改表格中“没有判为不适用项的数据”为“无” | √ |
|  | 5 安全问题风险评估 | 在测评项中需体现安全扫描、渗透测试发现的问题，安全问题风险评估后不再单独添加安全问题；  注：扫描、渗透测试发现的问题对应到测评项目中：   1. 系统或中间件补丁或版本问题对应“a)应遵循最小安装的原则，仅安装需要的组件和应用程序” 2. 注入类、信息泄露类等问题对应“d)应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求” | √ |
|  | 7 问题处置建议 | 问题不会导致**高风险**，问题建议合理 | √ |
| 问题描述没有缺失的情况，如XX设备 | √ |
|  | 附录A 被测对象资产 | 内容与系统调查表、方案一致，设备与拓扑图一致 | √ |
| √ |
|  | 附录A.1 物理机房 | 记录表中有**灾备**机房的，需要列出 | √ |
|  | 附录A.2 网络设备 附录A.3安全设备  附录A.4 服务器/存储设备  附录A.5 终端/现场设备 附录A.6 系统管理软件/平台 | **测评对象单台设备单独一行**，能够识别唯一设备，与测评选择结果对应（若存在大量同类型设备情况，系统构成部分同类设备可合并，同类型设备在备注中填写设备数量） | √ |
| 除了云平台中独立数据库设备（如RDS），数据库不单独列出  有单独控制端的存储设备需纳入  堡垒机、日志审计服务器作为安全设备  操作系统、业务应用软件等信息填写无误 | √ |
|  | 附录A.7 业务应用软件 | B/S架构的系统识别是否包含前后台 | √ |
| 应用范围能覆盖业务介绍 | √ |
|  | 附录A.8 数据类别 | 需包括**鉴别数据、管理数据和业务数据**，特殊情况在本表格说明 | √ |
|  | 附录A.9 安全相关人员 | 一个人多个角色时，**一个人一行**，联系方式：手机、直线电话或分机，需要能明确到个人 | √ |
|  | 附录A.10 安全管理文档 | 内容与系统调查表、方案一致 | √ |
|  | 附录C.4.4 其他系统和设备 | 修改为“本次测评未涉及其他系统和设备。” | √ |
|  | 附录C.11 其他安全要求指标 | 若无其他安全要求指标（如邮件专项），替换这一段为“本次测评未涉及其他安全要求指标。” | √ |
|  | 附录D 单项测评测评结果记录 | 测评记录内容与标准要求一致，描述准确，无明显前后矛盾的地方，不抄写标准要求 | √ |
| 测试记录中引用的文档名称与调查表等一致 | √ |
| 总体描述测评记录中未出现非本报告的内容，如其他单位、项目名称等 | √ |
| **扫描、渗透结果体现到测评记录** | √ |
|  | 附录D.11 其他安全要求 | 若无其他安全要求，本段修改为“本次测评未涉及其他安全要求” | √ |
|  | 附录E 漏洞扫描结果记录 | 扫描报告导入测评能手后生成，列出问题详细情况、问题验证截图  外网应用增加渗透测试报告  暴露在外网的高危问题已整改 | √ |
|  | 附录F 渗透测试结果记录 | 粘贴渗透测试报告 | √ |
|  | 附录H 云计算平台测评及整改情况 | 若被测对象为云租户，此处粘贴云计算平台测评报告  若被测对象未使用云计算技术，则删除 | √ |
|  | 附录I 大数据平台测评及整改情况 | 删除 | √ |
|  | 尾页 | 报告末尾增加“[本页以下无内容]” | √ |
|  | 格式符合性检查 | 页眉、页脚、报告编号、项目编号、字体、字号等准确，页脚最后页页码与总页码一致 | √ |
|  | 目录 | 所有内容修改完后更新目录 | √ |
|  | 机构编号 | 机构编号为0092 | √ |

注1:记录编号P开头的为项目编号；

注2;如果上述修改项多人检查，则确认人签名时分别标注检查的修改项编号。

注3：修改项有下划线的，表示是测评能手导出需要修改的项。

确认人/确认日期：