2018年度网络等级测评项目抽查问题分析及解决方法

李明，公安部信息安全等级保护评估中心

2018 抽查要求

调研类 [10]

- 调研信息完整
- 有重要性分析

方案类 [20]

- 与调研一致
- 有项目基本信息
- 有被测对象描述
- 关键内容
  - 指标与级别相符
  - 抽样合理
  - 网络拓扑图规范
  - 有漏洞扫描和渗透测试

报告类 [50]

- 对象与方案一致
- 测评记录清晰、翔实
- 符合性判断准确
- 有漏洞扫描和渗透测试结果
- 安全问题描述准确
  - 问题描述准确
  - 风险分析合理
  - 整体测评准确
- 测评结论准确
- 整改建议合理

质量控制 [10]

- 方案评审
  - 有评审记录
  - 记录内容完整
  - 意见有针对性
- 报告评审

规范性 [10]

- 原始记录签字
- 方案签字
- 报告格式符合要求

01 前期调研

主要问题：

1. 调研表格内容缺失
   - 缺少终端、中间件等对象
   - 未填写网络区域、版本等关键表项
   - 未填写应用处理流程(数据流)
2. 调研结果与实际情况不一致
   - 边界不完整，外联线路不明
   - 设备缺失，区域数量不符，属性错误

主要问题：

3. 定级对象与设备对应关系不清晰
4. 拓扑图不规范
   - 不清晰
   - 网络区域未标注
   - 设备未唯一标识
   - 多功能设备标注不当
5. 针对云平台、工控系统的调研不充分

原因分析：

1. 没有意识到充分调研的重要性
   - 指标、对象选择错误
   - 测评实施混乱，测评证据不完整
   - 测评结论不正确
2. 不了解表格的体系关系
   - 系统-业务-应用系统-主机-网络区域网络设备-安全设备
   - 应用系统软件处理流程/业务数据流程

原因分析：

3. 未实施调研，或调研与测评一起，或调研表格由委托方填报且未核对
4. 未按照拓扑图要求绘制，或图省事
5. 未针对云平台等新形态定制调研内容
   - 云租户 / 云平台
   - 虚拟设备(网络、主机、应用)
   - 云操作系统/云管理软件

解决方法及建议：

1. 重视调研环节；
2. 加强调研表格审查；
3. 细化调研表格，加强培训；
4. 表格间的关联关系（下图）：
   - 由定级对象入手，通过应用系统关联主机
   - 通过网络区域关联网络和主机设备
   - 通应用过系统处理流程/数据流程将终端、服务器和网络设备串联起来。

表 E.4　信息系统基本情况

填表人：　　日期：

序号	信息系统名称	安全保护等级	业务信息安全保护等级	系统服务安全保护等级	承载业务应用

表 E.5　信息系统承载业务(服务)情况

填表人：　　日期：

序号	业务(服务)名称	业务描述	业务处理信息类别	用户数量	用户分布范围	涉及的应用系统软件	是否 24 小时运行	是否可以脱离系统完成	重要程度	责任部门

表 E.10　服务器设备情况

填表人：　　日期：

序号	服务器设备名称	型号	物理位置	所属网络区域	IP 地址/掩码/网关	操作系统版本/补丁	安装应用系统软件名称	主要业务应用	涉及数据	是否设备	重要程度

表 E.6　信息系统网络结构(环境)情况

填表人：　　日期：

序号	网络区域名称	主要业务和信息描述	IP 网段地址	服务器数量	终端数量	与其连接的其他网络区域	网络区域边界设备	重要程度	责任部门	备注
1										
2										

表 E.6　信息系统网络结构(环境)情况

填表人：　　日期：

序号	网络区域名称	主要业务和信息描述	IP 网段地址	服务器数量	终端数量	与其连接的其他网络区域	网络区域边界设备	重要程度	责任部门	备注
1										

表 E.7　外联线路及设备端口(网络边界)情况

填表人：　　日期：

序号	外联线路名称（边界名称）	所属网络区域	连接对象名称	接入线路种类	传输速率（带宽）	线路接入设备	承载主要业务应用	备注

表 E.8　网络设备情况

填表人：　　日期：

序号	网络设备名称	型号	物理位置	所属网络区域	IP 地址/掩码/网关	系统软件及版本	端口类型及数量	主要用途	是否热备	重要程度	备注

表 E.9　安全设备情况

填表人：　　日期：

序号	网络安全设备名称	型号(软件/硬件)	物理位置	所属网络区域	IP 地址/掩码/网关	系统及运行平台	端口类型及数量	是否热备	备注

表 E.16　应用系统软件处理流程

填表人：　　日期：

应用系统软件处理流程图 （应用软件名称：　　）	应用系统软件处理流程图 （应用软件名称：　　）

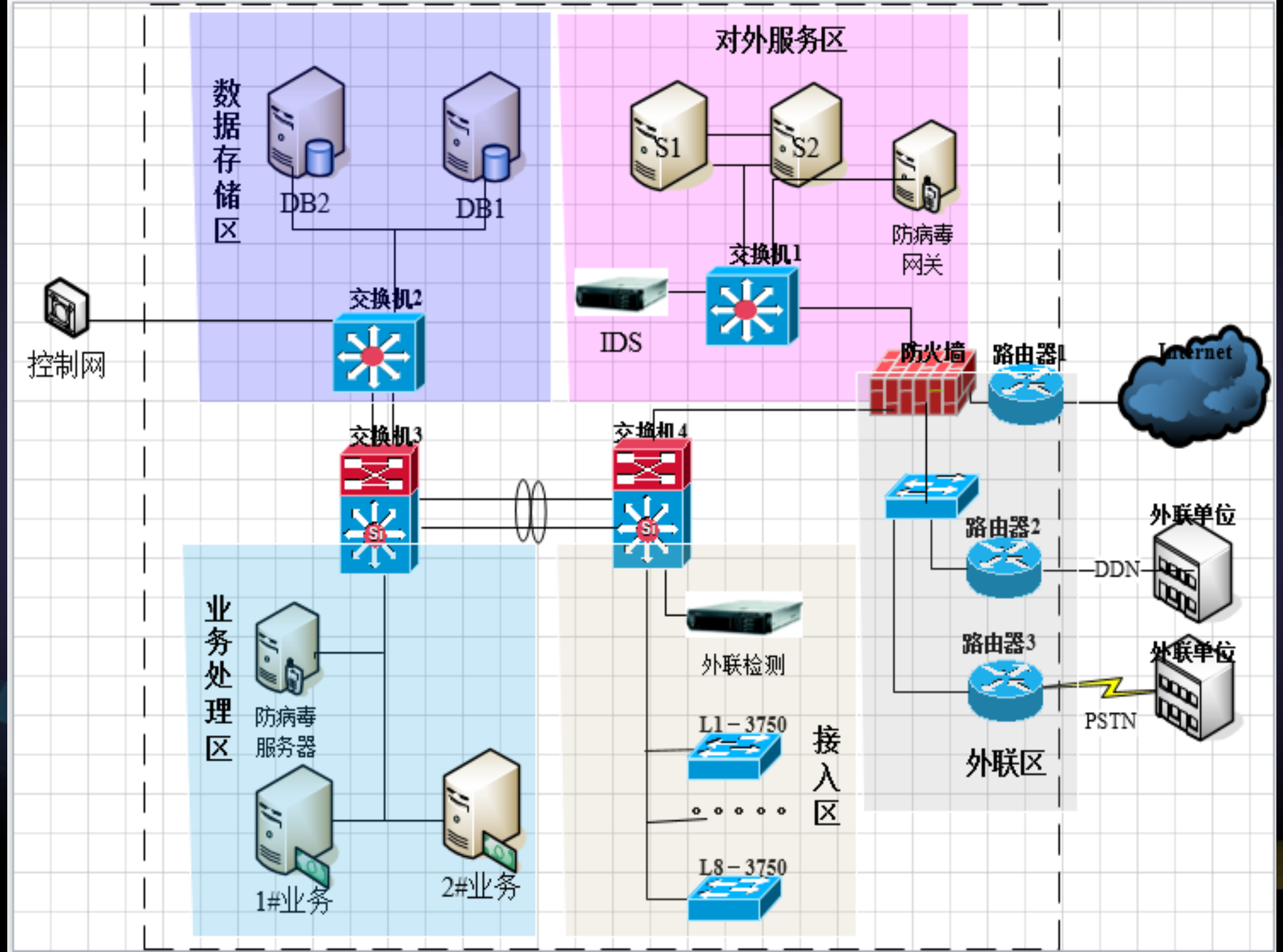
表 E.17　业务数据流程

填表人：　　日期：

数据流程图（数据名称：　　）	数据流程图（数据名称：　　）
注：重要数据应该描绘数据流程图，从数据产生到传输经过的主要设备，再到存储设备等流程。	

规范的拓扑图：

1. 布局由外到内，由上到下
2. 清晰标注区域，明确边界设备
3. 标注外联线路及互联系统
4. 标注各区域内设备/类型（含服务器和终端，名称唯一）
5. 与调研表内容比对一致。


数据存储区
DB2
DB1
对外服务区
S1
S2
防病毒网关
交换机1
IDS
控制网
交换机2
防火墙
路由器1
Internet
交换机3
交换机4
路由器2
外联单位
DDN
外联检测
路由器3
外联单位
PSTN
业务处理区
防病毒服务器
L1－3750
接入区
外联区
1#业务
2#业务
L8－3750

云计算环境：

1. 云客户系统 vs. 云服务平台
2. 云租户系统
   - 物理+虚拟 vs. 全虚拟
   - 承载平台名称、虚拟设备(网络、主机、安全)、应用系统等
3. 云计算平台
   - 提供的服务模式
   - 机房、硬件设备、云平台软件(虚拟化控制、运维、运营等)

02 测评方案

主要问题：

1. 测评依据不准确
   - GB/T 22239-2008
2. 缺少等级保护对象描述
   - 未明确安全保护等级
   - 直接给出抽选对象
3. 测评指标选择不合理、不准确
   - 缺少行业指标
   - 与定级结果不符合

主要问题:

4. 测评对象选择不合理
   - 对象类型不全面:终端、中间件
   - 抽样比例不合理(第三级不低于2台)
5. 工具测试有缺陷:
   - 接入点、路径不合理，对象不全面
   - 无渗透测试内容
   - 无风险揭示及规避措施。

原因分析：

- 《测评过程指南标准》掌握不足
- 未建立《测评方案》模版
- 调研不充分或有意简化内容
- 委托方不同意工具测试，或未掌握工具测试方法
  - 漏洞扫描接入点设置、扫描路径规划以及扫描对象选择；
  - 渗透测试接入点设置以及渗透测试内容。

解决方法与建议：

- 整体上
  - 建立测评方案模版；
  - 加强《测评实施指南》标准培训；
  - 重视方案评审，细化评审规则。

解决方法与建议：

- 测评依据
  - GB/T 22239-2008
  - GB/T 28448-2012
  - GB/T 28449-2012
  - GB/T 20984-2007
  - // 行业等级保护标准
  - 测评服务合同

解决方法与建议：

- 测评对象选择不合理：
  - 遍历业务路径找测评对，确保象测评对象类型要全面覆盖。
    - 运维终端，业务管理终端，中间件（独立安装运行）
  - 按照安全保护等级确定抽样比例（第三级不低于2台）。

解决方法与建议：

- 漏洞扫描
  - 参考终端部署及业务路径设置扫描接入点和扫描路径；
  - 确保象测评对象类型要全面覆盖，包括互联设备、安全设备、操作系统、数据库管理系统、中间件和应用系统等；
  - 面向操作系统的本地扫描作为主机安全检查的补充。
- 渗透测试
  - “准实战”vs.“指哪儿打哪儿”

03 测评报告

主要问题:

1. 结果记录照抄要求项;
2. 测试方法不全面，仅访谈
3. 缺失部分测评记录(有对象无记录，要求项部分内容)
4. 结果记录文不对题、前后矛盾
5. 结果记录未装订、无委托方确认，或无小签或跨签;

原因分析：

1. 无现场记录的考核管理机制
2. 对测评项理解不全面、不透彻，实际应用经验不足
3. 测评指导书实施步骤不详细
4. 实施人员进场时间不统一，未有效沟通
5. 项目配合人员提供情况不准确

解决方法与建议：

1. 加强测评记录规范化管理
2. 测评证据确认签字
3. 设立监督员对测评记录的完整性、准确性等进行监督和审核
4. 开展针对测评人员能力的持续培训

解决方法与建议：

1. 主机安全—访问控制—b)/c)中的权限分离，是特指“三权”分离，至少应实现审计权限分离，不是指网络设备管理中常见的用户权限分级；
2. 应用安全--抗抵赖—a)/b)，有报告将“数字证书进行身份鉴别”和传输加密这两个措施作为满足“提供数据原发或数据接收的功能”的证据，对标准条款的理解有误（GB/T 17903.1/2/3-2008）

解决方法与建议:

3. 应用安全--软件容错—b)款:应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复:较多的报告中的回答都是使用了双机系统，能够在故障发生时进行倒换恢复。

主要问题：

1. 测评报告抽查对象与方案不一致
2. 原始记录不同项之间自相矛盾
3. 原始记录与测评报告严重不符
4. 原始记录与测评报告严重不符
5. 滥用不适用项或不适用项说明不合理或报告前后不一致
6. 整体测评缺失或测评后未调整得分或描述前后矛盾

主要问题：

- 工具测试结果不放入
- 风险分析不合理；
- 测评结论不准确；
- 测评项作为整改建议，无具体指导性；或未结合系统实际情况，给出的建议不合理。

解决方法与建议：

- 强调要求必须使用新的等级测评报告模版，严格按照报告模版出具报告，不能缺失章节及内容；
- 建立单个测评项的评分标准，对于每一测评项，细化预期结果，并根据测评证据与预期结果的符合程度，分别给出0分、1分、2分、3分、4分、5分的情况；

解决方法与建议：

- 建立统一的风险分析方法，保证同一机构出具的风险分析结果保持一致；
- 建立技术沟通机制，对整体测评分析过的内容汇总形成技术积淀，为后续报告编写奠定技术基础；
- 加强报告评审把关，对报告内容和格式进行审核，对重要章节内容进行技术评审。

04 质量控制

质量控制问题：

1. 评审内容笼统
   - 对象抽选合理　　■具测试
2. 评审意见没有针对性
   - 根据意见进一步修订方案
3. 评审意见无结论
4. 评审信息不完整
   - 评审参与人角色/负责人签字

解决方法与建议:

- 修订模版:
  - 评审记录勾选与填空相结合;
  - 不符合项目要可追溯;
  - 结论是否通过要明确;
  - 修改意见要具体;
  - 参与信息要完整(编制组、评审组成员、评审负责人)。

05 规范性

规范性问题:

- 有签字无签章
- 报告未盖骑缝章
- 报告编号有误
- 未使用标准模版
  - 页眉去掉报告编号
  - 缺少特定章节