等保 2.0 重点汇总

1　整体测评结果分析从安全控制点间、区域间/层面间和验证测试等方面对单项测评的结果进行验证、分析和整体评价。根据整体测评结果，对安全问题汇总表中的安全问题进行修正，风险等级为“高”、“中”、“低”，修正后的问题风险程度，等级测评结论由综合得分和最终结论构成。

1. GB17859-1999《计算机信息系统安全保护等级划分准则》是网络安全领域唯一强制的标准，也是网络安全等级保护标准体系的中的基础标准。

2. GB17859-1999《计算机信息系统安全保护等级划分准则》将计算机信息系统的安全保护能力由低到高划分五个等级，分别第一级-用户自主保护级、第二级-系统审计保护级、第三级-安全标记保护级、第四级-结构化保护级、第五级-访问验证保护级。

3. GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》规定了网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求,适用于知道分等级的非涉密对象的安全建设和监督管理。

保护数据在存储、传输、处理过程中不被泄露、破坏和免受未侵权的修改的信息安全类要求（简记为 S）

保护系统连续正常的运行，免受对系统的未侵权的修改、破坏而导致系统不可用的服务保证类要求（简记为 A）

测评单元编码规则为三组数据，第一组：L1-5 级别，

第二组：

PES 为安全物理环境、

CNS 为安全通信网络、

ABS 为安全区域边界、

CES 安全计算环境、

SMC 为安全管理中心、

PSS 为安全管理制度、

ORS 为安全管理制度

HRS 为安全管理人员

CMS 为安全建设管理

MMS 为安全运维管理

BDS 代表大数据

数字代表应用场景，1 安全通用，2，云计算，3 移动互联 4 物联网 5 为工业控制系统

数据安全与备份恢复:主要测评对象包括加密机、VPN 设备、备份软/硬件系统以及灾备中心等。

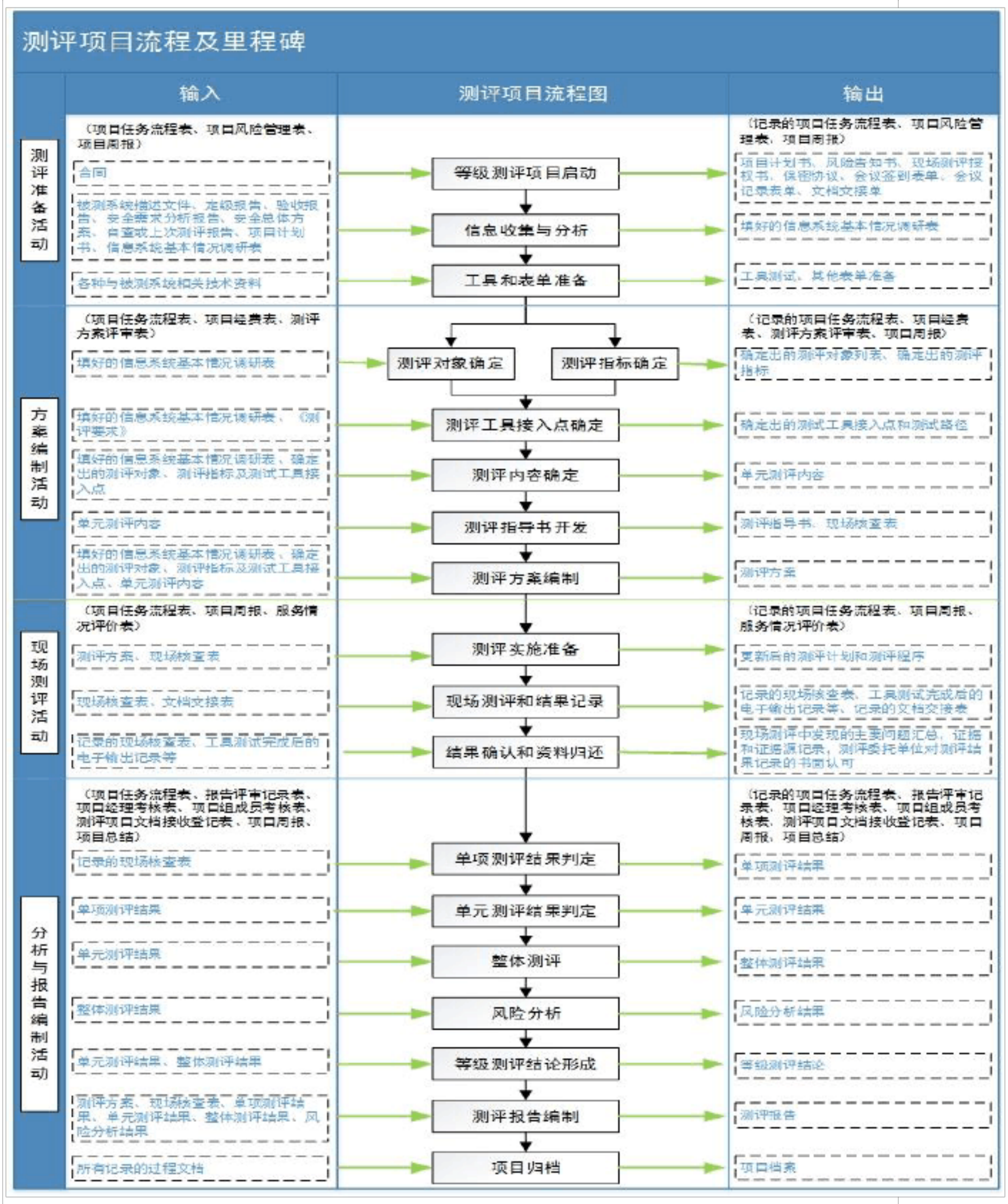
与《测评要求》的 10 个单元测评内容相对应，建议测评机构开发以下测评指导书。

- 物理安全：覆盖相关测评指标的物理安全测评指导书。
- 网络安全：网络安全整体测评指导书、路由器安全测评指导书（Cisco、华为）、交换机安全测评指导书（Cisco、华为）和防火墙安全测评指导书（天融信、联想网御等）。
- 主机安全：主机安全整体核查表、操作系统安全测评指导书（AIX 和 Windows Server）、数据库安全测评指导书（Oracle 和 SQL Server）、应用平台安全测评指导书（WebSphere 和 Weblogic）。
- 应用安全：网站应用安全测评指导书、E-mail 系统应用安全测评指导书、业务系统应用安全测评指导书等（具备基本内容，部分内容需针对具体应用进行细化和调整）。
- 数据安全与备份恢复：VPN 安全测评指导书、数据安全与备份恢复安全测评指导书，其内容可依据测评对象合并到网络安全、主机安全或应用安全的相应测评指导书中。
- 安全管理制度：安全管理制度测评指导书。
- 安全管理机构：安全管理机构测评指导书。
- 人员安全管理：人员安全测评指导书。
- 系统建设管理：安全管理制度测评指导书。
- 系统运维管理：系统运维管理测评指导书。
- 漏洞扫描指导书。

测评力度在广度方面主要体现为测评对象的类型和数量

风险的规避：

1.签署委托测评协议，2.签署保密协议，3.签署现场测评授权书 4.现场测评工作的风险规避，渗透需要测试环境 5.测评现场还原 6.规范化实施过程 ，7.沟通与交流



4）确定测评实施

测评实施是测评指导书的核心内容，由测评方法、操作步骤和结果记录三部分组成。测评方法（访谈、检查或测试）和操作步骤是由测评对象所在目标系统的安全保护等级决定，体现了与该安全保护等级相对应的测评努力程度，决定了测评人员及委托方对测评结果的信任程度。

题集：

1. 给一个网络拓扑图，结合 2.0 指出有哪些不足，给出整改方案

2. 工具测试流程：

1. 收集目标系统信息 2. 规划工具测试接入点 3. 编制《工具测试作业指导书》 4. 现场测试 5. 测试结果整理分析

2. 工具测试接入点：

1. 由低级别系统向高级别系统探测，

2. 同一系统同等重要程度功能区域之间要相互探测

3. 由较低重要程度区域向较高重要程度区域探测

4. 由外联接口向系统内部探测

5. 跨网络隔离设备要分段探测。

3. 算分题---2.0 算分需要搞懂

4. 测评方案，整体测评，测评对象选取

答：测评方案：决定等级测评项目实施成功与否的关键，根据测评准备活动中收到的被测定级对象的具体情况，选取测评对象和测评指标，选择测评方法，规划现场测评实施方案，为现场测评活动提供基本的文档和指导方案。测评方案内容包括项目概述、被测等级保护对象情况、测评对象与指标、测评方法与工具、工具测试、测评内容与实施以及配合资源要求。

测评对象的选取：重要性原则-抽查重要的服务器、数据库和网络安全设备，安全性原则-抽查对外暴露的网络边界　共享性原则-抽查共享设备和数据交换设备，全面性原则-抽查应尽量多的系统各种设备类型，操作系统类型，数据库类型，应用系统类型，符合性原则-选择的设备和软件系统应满足响应等级测评力度要求。在满足测评力度的前提下允许对系统构成组件进行抽查，一般等级对象可以采用分层抽样方法，复杂定级对象采用多阶抽样方法。1. 对定级对象构成组件进行分类，客户端、服务器、网络互联设备、安全设备、安全相关人员和安全

管理文档，在分类基础上继续细化。2.对于每一类定级对象构成组件，应根据调研结果进行重要性分析，选择对被测定级对象来说重要程度高的设备。再可进行物理位置分析、共享性分析和全面性峰分析，进一步完善测评对象集合；最后依据测评力度恰当性分析，综合衡量测评投入和结果产出，确定测评对象的种类和数量。

整体测评并举例：根据单项测评结果整体安全保护状况进行综合评价分析，分别从安全控制点测评、安全控制点间、层面间、和区域间四个角度相互作用分别进行测评，根据综合分析结果修正安全问题风险等级。例如机房未安装防盗报警设置，修正前风险等级，为中，修正理由描述为机房安排专人24小时值守，可起到防盗报警功能，windows服务器操作系统没有设置登陆失败功能，描述为所有登陆windows服务器的终端都是用KVM本地登录，登录终端设在机房，机房24小时专人值守，因此不存在外部人员利用终端远程登录猜解口令的危险，修正为低。

测评内容的确定：

从单项测评和整体测评，物理安全测评指标在机房和办公环境等对象上实现。网络安全测评指标在网络互联设备和安全设备上实现，主机安全测评指标主要在操作系统、数据库以及些操作系统和数据库的加固软件上。应用安全的测评对象是应用软件以及应用平台等。管理安全主要的测评对象是各种规章制度、操作规程、过程记录文档，访谈的运维管理人员等。测评内容确定任务的主要工作已确定的测评指标和测评对象结合起来，将测评指标映射到各个测评对象上，然后结合测评对象的特点，说明各测评对象所采取的测评方法。如此构成一个个可以具体实施测评的单元。

5. 风险赋值分析是什么？

采用风险分析方法分析等级测评结果中存在的安全问题可能对被测定级对象安全造成的影响，根据单项目测评结果被威胁利用可能性，威胁被利用后对系统造成的安全影响程度，综合被威胁利用的可能性和影响程度结果对系统面临的安全风险进行赋值。

6. 风险赋值的依据是什么？

危害分析和风险等级判定，风险分析结合关联资产和关联威胁分别分析安全问题可能产生的危害结果，找出可能对系统、单位、社会及国家造成的最大安全危害或损失风险等级。风险分析结果的判断综合了相关系统组件的重要程度、安全问题的严重程度、安全问题被关联威胁利用的可能性、所影响的相关业务应用以及发生安全事件可能的影响范围等因素。等级根据严重程度进一步确定为“高”、“中”、“低”。结合被测系统的安全保护等级对风险分析进行评价，对国家、社会和其他组织的合法权益造成的风险

1、测评可能造成的风险：

1)测评活动可能影响系统正常运行

需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机查看一

些信息，可能对系统的运行造成影响或存在误操作能。进行漏洞扫描测试、渗透能力测试。测试可能会对网络和系统的负载造成一定的影响，渗透测试还可能影响到服务器和系统正常运行。

2) 可能造成敏感信息泄露

可能因泄露使被测评系统面临威胁的敏感信息包括:网络拓扑、IP 地址、业务流程、安全机制、安全隐患和其他重要信息等。

2、中级测评师的能力要求：

熟悉信息安全等级保护相关政策、法规；

正确理解信息安全等级保护标准体系和主要标准内容，能够跟踪国内、国际信息安全相关标准的发展；

掌握信息安全基础知识，熟悉信息安全测评方法，具有信息安全技术研究的基础和实践经验；

具有较丰富的项目管理经验，熟悉测评项目的工作流程和质量管理的方法，具有较强的组织协调和沟通能力；

能够独立开发测评指导书，熟悉测评指导书的开发、版本控制和评审流程；

能够根据信息系统的特点，编制测评方案，确定测评对象、测评指标和测评方法；

具有综合分析和判断的能力，能够依据测评报告模板要求编制测评报告，能够整体把握测评报告结论的客观性和准确性。

了解等级保护各个工作环节的相关要求。

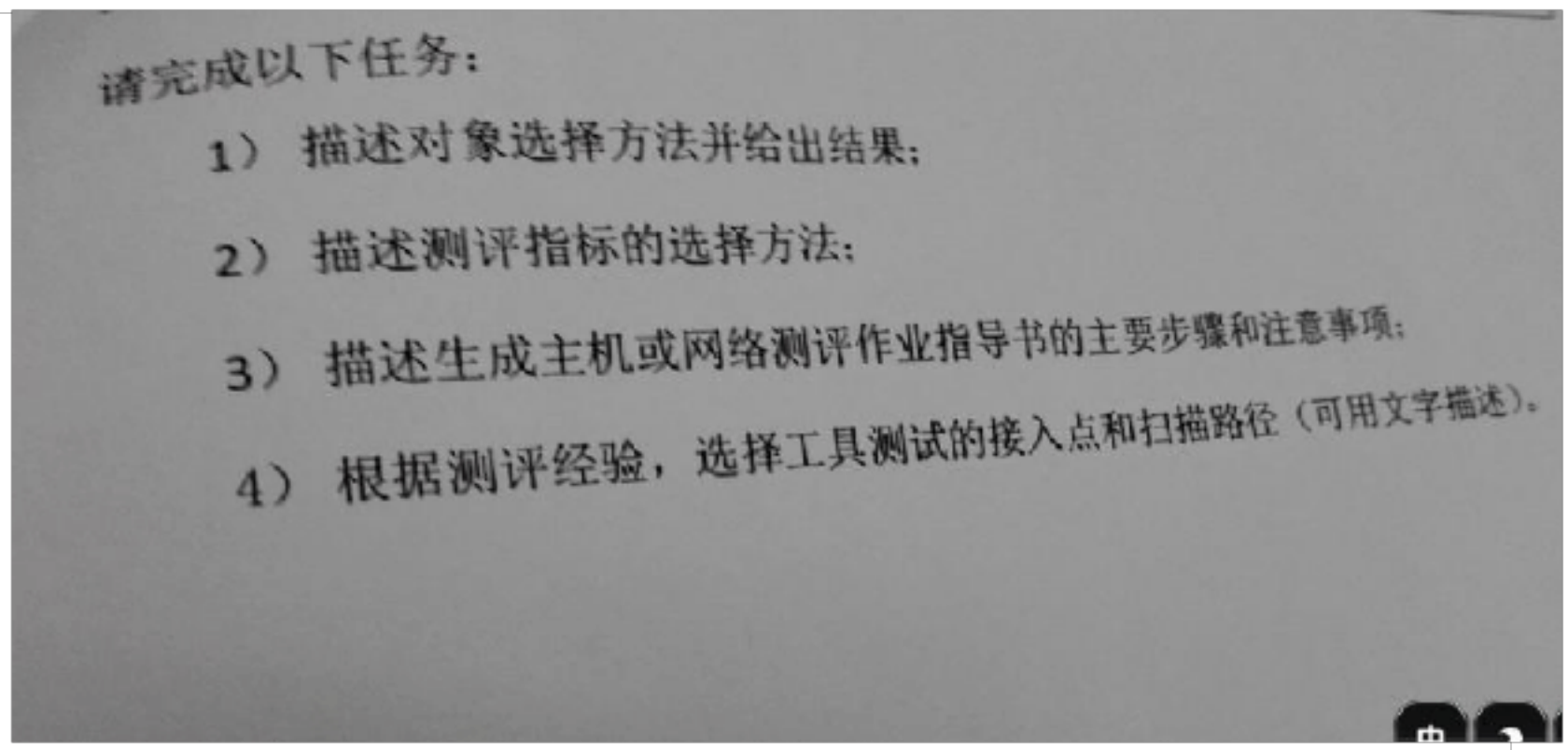
能够针对测评中发现的问题，提出合理化的整改建议。

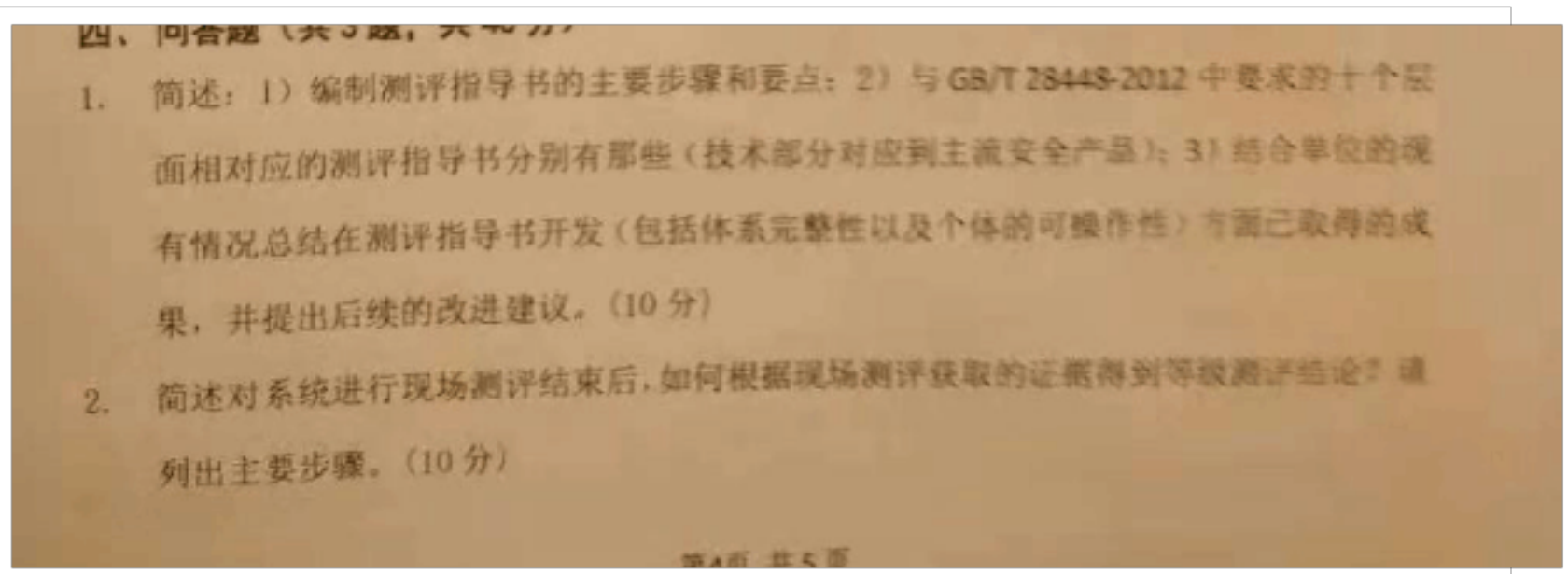
3 、（GB/T 28449-2012 测评过程指南　附录 D）

1） 测评对象选择的原则，并根据他给的图和提示，画测评对象选择的表格

2） 网络层面的安全问题并给出实现安全机制，画拓扑图

3）算控制项分数

7. 

8. 

9. 如何根据现场测评获取的证据的到等级测评结论？

单项测评结果判定汇总-整体测评结果分析-安全问题风险分析-找出系统保护现状与等级保护基本要求之间的差距，并根据等级测评结论判定原则形成等级测评结论，等级测评结论由综合得分和最终结论构成。

10. 48期好像有这个题
在主机测试前期调研活动中，收集信息的内容（至少写出六项）？在选择主机测评对象时应该注意哪些要点?
答：至少需要收集服务器主机的设备名称、型号、所属网络区域、操作系统版本、IP地址、安装的应用软件名称、主要业务应用、涉及数据、是否热备、重要程度、责任部门。
测评对象选择时应该注意 重要性、代表性、完整性、安全性、共享性五大原则。

11. 3、给个网络拓扑图和设备调查表给你，让你写网络设备的测评指标（控制点）；写要开发什么测评指导书；画测试接入点并说明；

12. 【路人】河南-O(972182914) 2018-10-26 11:01:30 查看前后消息
48中级大题1，测评指导书编写注意事项，十块指导书中详细描述网络安全设备主流厂家指导书，以及改进建议
2，如何得出等级测评结论
3，指出给出的网络拓扑图中的5处错误并给出整改建议，最后画出整改后的拓扑图
应该是这些 记忆力不行见谅

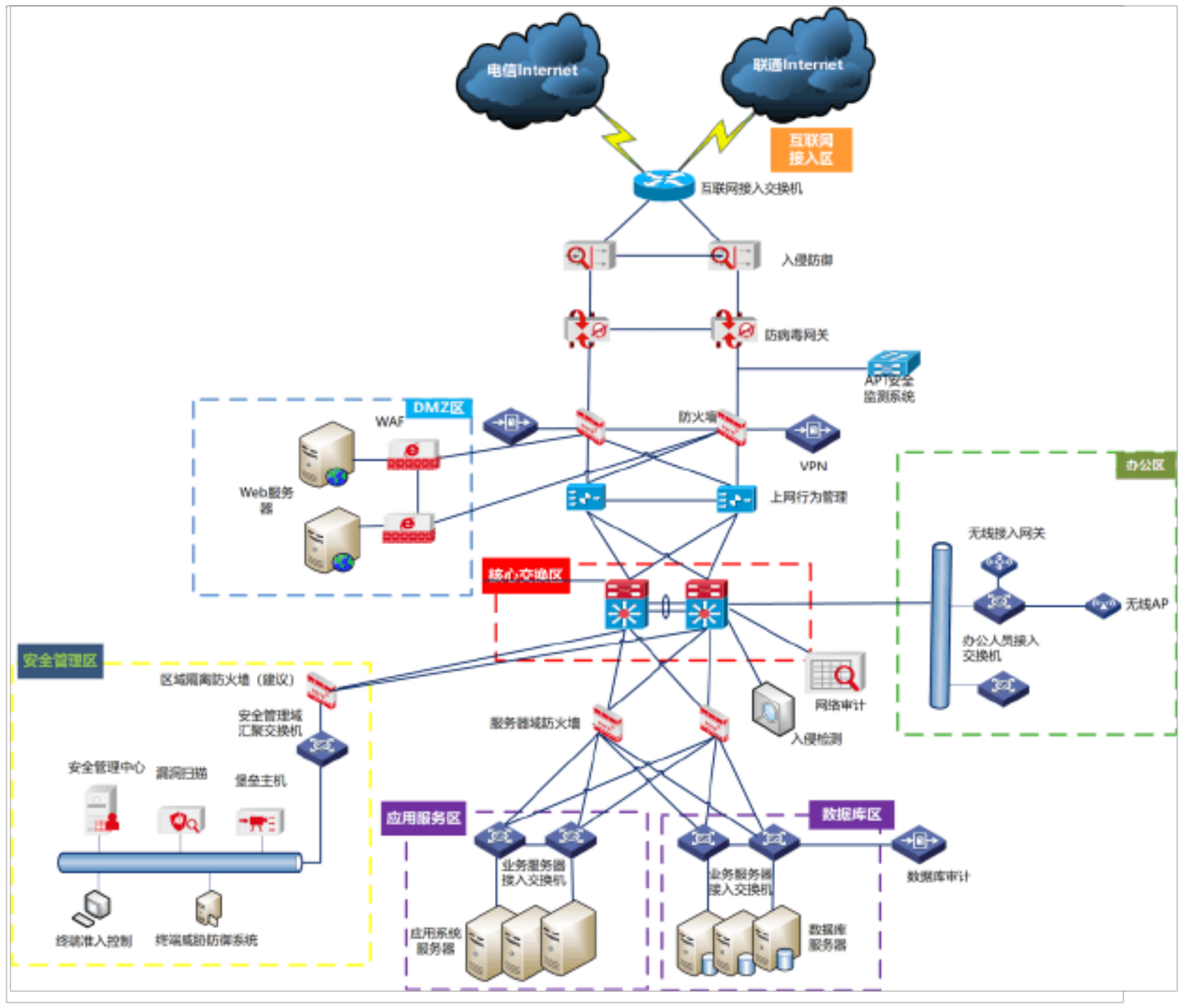
1. 测评指标选择依据 **2.0** 标准，然后举例说明：

答：《基本要求》是等级测评依据的主要标准，1，测评指标来源于标准对不同安全保护等级定级对象的基本要求 2.依据定级情况确定定级对象应采取的安全保护措施 SAG 组合情况，并从基本要求的安全要求中选择相应等级的安全要求作为测评指标 3 为针对不同被测定级对象的测评指标。根据定级对象展现形态，采取不同的测评指标选择方法，在选择测评指标时，所有定级对象都应从“安全通用要求”中选择相应等级的安全要求作为测评指标的一部分，同时还应根据定级对象的展现形态从不同的“安全扩展要求”类中选择相应等级的安全扩展要求作为测评指标的一部分。

2. 举例：某给予云计算技术构建的定级对象的定级为系统安全保护等级为 3 级，业务信息安全保护等级为 3 级，系统服务安全保护等级为 2 级，则该定级对象所有测评对象的测评指标集合将包括《基本要求》“安全通用要求”中的 **3** 级通用指标类（**G3**）**.3** 级业务信息安全性指标类 **S3,2** 级业务服务保证性指标 **A2,** 以及第三级“云计算安全扩展要求”中所有指标类。

二、云数据存放在云平台中可能存在的问题以及处理措施：

三、依据 2.0 标准，根据说出来的区域进行拓扑图设计，画拓扑图和文字描述：



网络架构：

e） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。	网络拓扑	应做到关键网络设备、安全设备和关键计算设备的硬件冗余（主备或双活等）和通信线路冗余；

可信验证：

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。	提供可信验证的设备或组件、提供集中审计功能的系统	1）基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用 程序等进行可信验证； 2）在应用程序的关键执行环节进行动态可信验证； 3）当检测到通信设备的可信性受到破坏后能够进行报警； 4）以审计记录的形式送至安全管理中心。

边界防护：（非法内联、非法外联、限制无线网络）部署准入系统。

b） 应能够对非授权设备私自联到内部网络的行为进行 检查或限制 ；	终端管理系统或相关设备	1）采用技术措施防止非授权设备接入内部网络； 2）所有路由器和交换机等相关设备闲置端口是否均已关闭。
c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制 ；	终端管理系统或相关设备	采用技术措施防止内部用户存在非法外联行为；
d） 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。	网络拓扑和无线网络设备	1）无线网络的部署方式，是否单独组网后再连接到有线网络； 2）无线网络通过受控的边界防护设备接入到内部有线网络。

入侵防范：
抗 **APT** 攻击系统、网络回溯系统、威胁情报检测系统、抗 DDoS 攻击系统和入侵保护系统或相关组件
恶意代码防范：
防病毒网关和 UTM 等提供防恶意代码功能的系统或相关组件；
防垃圾邮件网关：防垃圾邮件网关等提供防垃圾邮件功能的系统或相关组件；
身份鉴别：网络设备、安全设备、操作系统、数据库、应用，双因子（采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；）
强制访问控制：针对操作系统、数据库和应用。

f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	应核查访问控制策略的控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录或字段级；