**等级保护题库**

1. **单选题**
2. 在等保1.0的基本要求中，网络设备防护的内容归属于网络安全，在等保2.0中将其归属到（）？

A 安全通信网络

B 安全区域边界

C 安全计算环境

D 安全管理中心

答案：c

1. 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由（）担任或授权。

A 系统管理员

B 安全管理员

C 技术负责人

D 单位主管领导

答案 D

1. 在保证各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互，是指的（）技术？

A 强制访问控制

B 可信计算

C 结构化保护

D 多级互联

答案 D

1. 在（）级系统安全保护环境中开始要求使用强制访问控制？

A 一

B 二

C 三

D 四

答案 C

1. 在（）中规定了计算机系统安全保护能力的五个等级

A 《计算机信息系统安全保护等级划分准则》

B 《信息安全技术 网络安全等级保护定级指南》

C 《信息安全技术 网络安全等级保护基本要求》

D 《信息安全技术 网络安全等级保护测评要求》

答案 A

1. 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行（）次检测评估。

A 一

B 二

C 三

D 四

答案 A

1. 关键信息基础设施的安全保护等级应不低于等保（）

A 第一级

B 第二级

C 第三级

D 第四级

答案 c

1. 对于三级系统安全管理要求中，以下哪个控制点不属于安全运维管理方面要求（）.

A 环境管理

B 介质管理

C 服务供应商选择

D 变更管理

答案 c

1. 三级系统应按照等保2.0要求采用密码技术保证通信过程中数据的（）.

A 完整性

B 保密性

C 可用性

D 可控性

答案 B

1. 信息系统遭到破坏后，会对国家安全造成一般损害的，应定为（）？

A 一

B 二

C 三

D 四

答案 c

1. 在等保2.0中，以下测评结论与判定依据描述正确的是？

A 被测对象中存在安全问题，但不会导致被测对象面临中、高等级安全风险，且系统综合得分90分以上（含90分）的，判定为优。

B 被测对象中存在安全问题，但不会导致被测对象面临高级安全风险，且系统综合得分70分以上（含70分）的，判定为良。

C 被测对象中存在安全问题，而且会导致被测对象面临高等级安全风险，或被测对象综合得分低于70分的，判定为中。

D 被测对象中存在安全问题，但不会导致被测对象面临高等级安全风险，且系统综合得分80分以上（含80分）的，判定为差。

答案 A

1. 网络安全等级保护基本要求安全管理中心层面，集中管控要求，三级系统审计记录的留存时间至少（）

A 一个月

B 二个月

C 三个月

D 六个月

答案 D

1. 三级安全通信网络-网络结构：应避免将重要网络区域部署在边界处，（）之间应采取可靠的技术隔离手段。

A 管理网络区域与其它网络区域

B 业务网络区域与其它网络区域

C 重要网络区域与其它网络区域

D 管理网络区域与业务网络区域

答案 c

1. 应只有在（）授权下，云服务商或第三方才具有云服务客户数据的管理权限。

A 云服务客户

B 云代理商

C 政府机关

D 云运营商

答案 A

1. 等保2.0中，不属于双因子鉴别的是（）

A 口令+验证码

B 口令+人脸识别

C 口令+令牌

D 口令+指纹

答案 A

1. 以下不属于等保测评常用方法的是？

A 调研访谈

B 确定定级对象

C 查看资料

D 技术测试

答案 B

1. 以下不属于等级保护定级流程的是？

A 确定定级对象

B 初步确定等级

C 公安机关评审

D 最终确定等级

答案 c

1. 安全通信网络安全控制点不包括（）

A 网络架构

B 访问控制

C 可信验证

D 通信传输

答案 B

1. 等保2.0三级系统要求，应与被录用人员签署保密协议，与关键岗位人员签署（）。

A 岗位责任协议

B 权限归属协议

C 岗位薪资保密承诺

D 以上全部

答案 A

1. 等保2.0三级系统，机房供电线路上需要安装（）和过电压防护设备保护装置，防止电力波动对电子设备造成损害。

A 电流稳压器

B 分流器

C 电流表

D 电压表

答案A

1. 定级对象的系统的必备特征不包括？

A 定级主体具有一定的经济实力

B 具有确定的主要安全责任单位

C 承载相对独立的业务应用

D 具有信息系统的基本要素

答案 A

1. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）正式发布的时间为？

A 2019年5月13日

B 2019年6月13日

C 2019年5月12日

D 2019年6月12日

答案 A

1. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）正式实施的时间为？

A 2019年11月12日

B 2019年11月2

C 2019年12月11日

D2019年12月1日

答案 D

1. 以下哪项属于等保测评存在的误区？

A 系统已上云或托管，仍需要做等保

B 系统定级越低越好

C 系统在内网，仍需要做等保

D 等保工作需要根据具体的国家标准、行业规定，安排合理的评测时间

答案 B

1. 《网络安全等级保护条例》的第二十二条和第二十三条明确指出（）网络应当按照网络安全等级保护有关标准规范，进行安全性测试、网络安全等级测试。

A 第一级网络和第二级

B 第二级网络和第三级

C 第三级网络和第四级

D 第四级网络和第五级

答案 B

1. 根据等级保护相关管理文件，等级保护对象的安全保护等级分为几级？

A 三级

B 四级

C 五级

D 六级

答案 C

1. 信息系统遭到破坏后，会对国家安全造成一般损害的，应定为（）？

A 第一级

B 第二级

C 第三级

D 第四级

答案 c

1. **判断题**
2. 对于三级系统进行更改设备基本配置信息时不需要纳入变更范畴，需要及时将配置信息库更新。

A 正确

B 错误

答案 B

1. 等级保护2.0三级系统测评合格最低分为60分。

A 正确

B 错误

答案 B

1. 当远程管理云计算平台中设备是，管理终端和云计算平台之间应建立单项身份认证机制。

A 正确

B 错误

答案 B

1. 审计管理员是管理系统中负责配置系统审计行为和管理系统审计信息的角色，审计管理员本身的操作行为，不用再进行审计记录。

A 正确

B 错误

答案 B

1. 被测系统应保证网络设备的业务处理能力满足业务高峰期需要。

A 正确

B 错误

答案 A

1. 等保2.0安全扩展要求包括云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制系统安全扩展要求、大数据安全扩展要求？

A 正确

B 错误

答案 A

1. 应该查云计算平台和云计算平台承载的业务应用系统相关定级备案材料，云计算平台安全保护等级是否不高于其承载的业务应用系统安全保护等级。

A 正确

B 错误

答案 B

1. 三级系统中，被测单位应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

A 正确

B 错误

答案 A

1. 安全建设管理测评层面中包括了定级和备案、产品采购和使用、自行软件开发、外包软件开发、工程实施、系统交付、服务供应商选择等控制点。

A 正确

B 错误

答案 A

1. 等保2.0定级指南，是GBT22240-2008？

A 正确

B 错误

答案 B

1. 关键信息基础设施和等级保护之间的关系，关键信息基础设施在等级保护第二级对象中确定。

A 正确

B 错误

答案 B

1. 等保备案机关最基层调整到县级以上公安机关。

A 正确

B 错误

答案 A

1. 一般等级保护建设的流程包括定级、备案、建设整改、等级测评、监督检查。

A 正确

B 错误

答案 A

1. 网络安全法第二十一条，规定国家实行网络安全等级保护制度。

A 正确

B 错误

答案 A

1. 等级保护有6个安全保护级别？

A 正确

B 错误

答案 **B**

1. 等保2.0已发布的核心标准有基本要求、设计指南、测评指南？

A 正确

B 错误

答案 B

1. 云平台系统是否可以作为定级对象？

A 正确

B 错误

答案 A

1. 未按《网络安全法》要求履行网络安全等级保护义务，关键信息基础设施运营者每年未开展过检测评估，有关部门警告后拒不整改或造成危害后果的，进行罚款（单位1万以上100万以下，责任人5000以上10万以下）、拘留、暂停业务等处罚；造成严重后果的根据《刑九》处三年以下有期徒刑、拘役或者管制。

A 正确

B 错误

答案 A

1. 在三级安全管理，安全运维管理层面，“环境管理控制点”要求应指定专门的部门或人员负责办公环境的管理。

A 正确

B 错误

答案 B

1. 等级保护中的高风险项是指等保测评时可以一票否决的问题，出现一个，则结论为差（不符合）。

A 正确

B 错误

答案 A

1. 网络运营者应当在规划设计阶段确定网络的安全保护等级。第二级以上网络运营者应当在网络的安全保护等级确定后15个工作日内，到县级以上公安机关备案。

A 正确

B 错误

答案 B

1. 三级系统应对数据库管理系统应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

A 正确

B 错误

答案 A

1. 在等保测评时会发现网络的技术措施的不足、安全管理制度不完善或缺失问题、系统漏洞、设备缺失或不足等问题；最终判定为高风险的问题，可视具体情况，择期整改即可。

A 正确

B 错误

答案 B

1. 等级保护定级中的SAG的具体含义是，S为业务信息对应的等级；A为系统服务对应的等级;G为通用安全等级，取S和A中最高等级。

A 正确

B 错误

答案 A

1. 等保测评常用方法中的查看配置，是指物理环境观察、逻辑结构和物理部署的对比观察。

A 正确

B 错误

答案 B

1. 本单位系统托管到外单位云平台或网络平台的，本单位作为系统的所有者或管理者，仍是责任主体，所以同样承担责任和义务；被托管单位作为网络服务提供者，承担相应责任和义务。

A 正确

B 错误

答案 A

1. 等保测评常用方法中的查看资料调研访谈，是指业务访谈、资产访谈与确认、安全技术访谈、安全管理访谈等。

A 正确

B 错误

答案 B

1. **多选题**
2. 等级保护工作有哪些规定动作（）？

A 定级

B 备案

C 建设整改

D 等级测评

E 监督检查

答案 ABCDE

1. 在等保2.0中，等保保护对象包括哪些？（）

A 信息系统

B 基础信息网络

C 工业控制系统

D 大数据平台

E 物联网

F 云计算平台

答案 ABCDEF

1. 新的等级保护标准重点强调的关键技术包括（）？

A 可信计算技术

B 强制访问控制

C 审计追查技术

D 结构化保护技术

E 多级互联技术

答案 ABCDE

1. 在等保里，一般我们指的三权分立指的是哪三权（）？

A 系统管理

B 安全管理

C 网络管理

D 审计管理

答案 ABD

1. 等保2.0安全通信网络层面三级系统应提供（）、（）和（）的硬件冗余，保证系统的可用性。

A 通信线路

B 系统

C 关键网络设备

D 关键计算设备

答案 ACD

1. 以下属于等级保护1.0与等级保护2.0的主要区别的有：

A 名称上的变化

B 保护对象有扩展

C 控制措施分类不同

D 通过结论变化

E 测评方法有变化

答案 ABCD

1. 等保测评存在的误区有哪些？

A 系统已上云或托管，就不用做等保了

B 系统定级越低越好

C 等保工作做测评就可以

D 等保测评做过一次就可以了

E 系统在内网，不需要做等保

答案 ABCDE

1. 等保测评流程包括哪些？

A 测评准备活动：工作启动、信息收集与分析、工具和表单准备

B 方案编制活动：测评对象确定、测评指标确定、测评工具测试方法确定、测评内容确定、测评指导书开发、测评方案编制

C 现场测评活动：现场测评准备、现场测评和结果记录、结果确认和资料归还

D 分析与报告编制活动：单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成、测评报告编制

答案 ABCD

1. 下列哪种技术手段可以测试和验证网络设备和安全设备的业务处理能力。（）

A 综合网管平台

B 登录设备查看相关配置

C 访谈网络管理员

D 设备的配置文档

答案 AB

1. 等保2.0安全区域边界层面访问控制应对（）等进行检查，以允许/拒绝数据包进出。

A 源目地址

B 源目端口

C 协议

D 访问控制策略

答案 ABC

1. 应在三级工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的（）等通用网络服务。

A E-Mail

B WEB

C Snmp

D tcp

E E、Telnet

F F、ftp

答案 ABEF

1. 等保测评常用方法中的查看资料包括：

A 管理制度的详细分析

B 管理策略的详细分析

C 管理制度的对标分析

D 管理策略的对标分析

E 管理制度的风险分析

F 管理策略的风险分析

答案 ABCD

1. 等保2.0第三级安全管理要求”人员配备”测评实施中的要求至少配备一定数量的（）。

A 系统管理员

B 审计管理员

C 安全主管

D 安全管理员

答案 ABD

1. 被测机房应采取措施防止感应雷，例如设置（）等。

A 避雷针

B 防雷保安器

C 避雷线

D 过压保护装置

答案 BD

1. 网络安全等级保护测评工作应由网络运营者主导，测评和运维等机构配合。其中网络运营者包括？

A 网络的所有者

B 管理者

C 网络的运维者

D 网络服务提供者

答案 ABCD

1. 网络安全等级保护主要标准有哪些？

A GB 17859-1999《信息安全技术 计算机信息系统安全保护等级划分准则》

B GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

C GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》

D GB/T 28449-2018《信息安全技术 网络安全等级保护测评过程指南》

E GB/T 20984-2007《信息安全技术 信息安全风险评估规范》

F GB/T 25070-2019《信息安全技术 网络安全等级保护安全设计技术要求》

答案 ABCDEF

1. 物联网分为哪些层？

A 现场控制层

B 感知层

C 网络传输层

D 处理应用层

答案 BCD

1. 第三级安全管理要求中，以下（）控制点不属于“安全管理机构”测评层面。

A 岗位设置

B 安全意识教育和培训

C 评审与修订

D 授权和审批

答案 BC

1. 等保2.0三级系统，应该查是否部署了具备运行状态监测功能的系统或设备，能够对（）的运行状况进行集中监测。

A 网络链路

B 安全设备

C 网络设备

D 服务器

答案 ABCD

1. 三级安全要求中入侵防范包括（）。

A 应遵循最小安装原则，仅安装需要的组件和应用程序。

B 应关闭不需要的系统服务、默认共享和高危端口。

C 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

D 应能够检测到重要节点进行入侵的行为，当发生严重入侵行为时进行日志记录即可，可以不提供报警。

答案 ABC

1. 等保2.0中所提出的“一个中心，三重防护”中的三重防护是（）？

A 通信网络防护

B 区域边界防护

C 重要数据防护

D 计算环境防护

答案 ABD

1. 等保2.0三级系统可基于可信根对通信设备的系统（）、（）、重要配登参数和（）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。

A 引导程序

B 系统程序

C 应用程序

D 通信应用程序

答案 ABD

1. 等保2.0建设核心思想包括（）？

A 以可信认证为基础，构建一个可信的业务系统执行环境

B 以访问控制技术为核心，实现主体对客体的受控访问

C 构建集中管控、最小权限管理与三权分立的管理平台

D 以安全监控为重点目标，仅重点系统强调安全防护理念

答案 ABC

1. 移动互联安全扩展要求提出特殊保护要求，增加的内容包括（）？

A 无线接入点的物理位置

B 移动终端管控

C 移动应用管控

D 移动应用软件采购

E 移动应用软件开发

答案 ABCDE

1. 工业控制系统信息安全主要思想包括哪些体系（）？

A 安全防护检测体系

B 安全态势分析体系

C 云服务体系

D 攻击溯源分析体系

答案 ABC

1. 等保2.0技术要求包括的控制类包括（）？

A 安全物理环境

B 安全通信网络

C 安全区域边界

D 安全计算环境

E 安全管理中心

F 安全管理制度

答案 ABCDE