CISP练习题三

你好

答题人

100

总分100

100

答对

共100题

答题解析 ⌃

全部题目 错题集

姓名：

你好

一、单项选择题。（每题1分，共100题，合计100分）

1、信息安全等级保护分级要求，第三极适用正确的是：（） 分值1分

○ A. 适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益

● B. 适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害

○ C. 适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害

○ D. 适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害

回答正确 +1分

2、下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求：（） 分值1分

○ A. 国家秘密及其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关机关规定

○ B. 各级国家机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级具体范围的规定确定密级

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● C. 对是否属于国家机密和属于何种密级不明确的事项，可由各单位自行参考国家要求确定和定级，然后报国家保密工作部门确定

○ D. 对是否属于国家秘密和属于何种密级不明确的事项。由国家保密工作部门，省、自治区、直辖市的保密工作部门。省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定。

回答正确 +1分

3、为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和 其他组织的合法权益，促进经济社会信息化健康发展，加强在中华人民共和国境内建设、 运营、维护和使用网络，以及网络安全的监督管理。2015 年6 月，第十二届全国人大常委 会第十五次会议初次审议了一部法律草案，并于7 月6 日起在网上全文公布，向社会公开 征求意见，这部法律草案是（） 分值1分

○ A.《中华人民共和国保守国家秘密法（草案）》

● B.《中华人民共和国网络安全法（草案）》

○ C.《中华人民共和国国家安全法（草案）》

○ D.《中华人民共和国互联网安全法（草案）》

回答正确 +1分

4、为了进一步提高信息安全的保障能力和防护水平，保障和促进信息化建设的健康发展，公安 部等四部门联合发布《关于信息安全等级保护工作的实施意见》（公通字[2004]66号），对等级保护工作的开展提供宏观指导和约束。明确了等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责分工等。关于该文件，下面理解正确的是（） 分值1分

● A. 该文件是一个由部委发布的政策性文件，不属于法律文件

○ B. 该文件适用于2004 年的等级保护工作。其内容不能约束到2005 年及之后的工作

○ C. 该文件是一个总体性指导文件，规定了所有信息系统都要纳入等级保护定级范围

○ D. 该文件适用范围为发文的这四个部门，不适用于其他部门和企业等单位

回答正确 +1分

5、自2004 年1 月起，国内各有关部门在申报信息安全国家标准计划项目时，必须经由以下哪个组织提出工作情况，协调一致后由该组织申报。（） 分值1分

○ A. 全国通信标准化技术委员会（TC485）

● B. 全国信息安全标准化技术委员会（TC260）

○ C. 中国通信标准化协会（CCCA）

○ D. 网络与信息安全技术工作委员会

回答正确 +1分

6、安全管理体系，国际上有标准（Information technology Security techniques Infor

mation systems ） （ISO/IEC 27001:2013），而我国发布了《信息技术信息安全管理体系要求》（GB/T 22080-2008）.请问，这两个标准的关系是（） 分值1分

- A. IDT （等同采用），此国家标准等同于该国际标准，仅有或没有编辑性修改
- B. EQV （等效采用），此国家标准等效于该国家标准，技术上只有很小差异
- C. AEQ （等效采用），此国家标准不等效于该国家标准
- D. 没有采用与否的关系，两者之间版本不同，不应直接比较

回答正确 +1分

7、“CC”标准是测评标准类的重要标准，从该标准的内容来看，下面哪项内容是针对具体的被 测评对象，描述了该对象的安全要求及其相关安全功能和安全措施，相当于从厂商角度制定 的产品或系统实现方案（） 分值1分

- A. 评估对象（TOE）
- B. 保护轮廓（PP）
- C. 安全目标（ST）
- D. 评估保证级（EAL）

回答正确 +1分

8、分组密码算法是一类十分重要的密码算法，下面描述中，错误的是（） 分值1分

- A. 分组密码算法要求输入明文按组分成固定长度的块
- B. 分组密码算法每次计算得到固定长度的密文输出块
- C. 分组密码算法也称为序列密码算法
- D. 常见的DES、IDEA 算法都属于分组密码算法

回答正确 +1分

9、密码学是网络安全的基础，但网络安全不能单纯依靠安全的密码算法，密码协议也是网络安全的一个重要组成部分。下面描述中，错误的是（） 分值1分

- A. 在实际应用中，密码协议应按照灵活性好、可扩展性高的方式制定，不要限制和框住所有的执行步骤，有些复杂的步骤可以不明确处理方式
- B. 密码协议定义了两方或多方之间为完成某项任务而制定的一系列步骤，协议中的每个参与方都必须了解协议，且按步骤执行
- C. 根据密码协议应用目的的不同，参与该协议的双方可能是朋友和完全信任的人，也可能是敌人和互相完全不信任的人
- D. 密码协议(cryptographic protocol),有时也称安全协议(securityprot ocol)，是使用密码学完成某项特定的任务并满足安全需求，其目的是提供安全服务

回答正确 +1分

10、美国计算机协会(ACM)宣布将2015 年的ACM 奖授予给Whitfield Diffic 和Wartfield

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

下面哪项工作是他们的贡献（） 分值1分

- A. 发明并第一个使用C 语言
- B. 第一个发表了对称密码算法思想
- C. 第一个发表了非对称密码算法思想
- D. 第一个研制出防火墙

回答正确 +1分

11、虚拟专用网络(VPN)通常是指在公共网络中利用隧道技术，建立一个临时的、安全的网络。 这里的字母P 的正确解释是（）。 分值1分

- A. sPccial-purpose,特定的、专用用途的
- B. Proprietary,专有的、专卖的
- C. Private,私有的、专有的
- D. sPecific,特种的、具体的

回答正确 +1分

12、为防范网络欺诈确保交易安全，网银系统首先要求用户安全登录，然后使用“智能卡+短信认证”模式进行网上转账等交易。在此场景中用到下列哪些鉴别方法？ （）
分值1分

- A. 实体“所知”以及实体“所有”的鉴别方法
- B. 实体“所有”以及实体“特征”的鉴别方法
- C. 实体“所知”以及实体“特征”的鉴别方法
- D. 实体“所有”以及实体“行为”的鉴别方法

回答正确 +1分

13、实体身份鉴别一般依据以下三种基本情况或这三种情况的组合：实体所知的鉴别方法、实体所有的鉴别方法和基于实体特征的鉴别方法。下面选项中属于实体特征的鉴别方法是（） 分值1分

- A. 将登录口令设置为出生日期
- B. 通过询问和核对用户的个人隐私信息来鉴别
- C. 使用系统定制的、在本系统专用的IC卡进行鉴别
- D. 通过扫墙和识别用户的脸部信息来鉴别

回答正确 +1分

14、常见的访问控制模型包括自主访问控制模型、强制访问控制模型和基于角色的访问控制模型 等。下面描述中错误的是（） 分值1分

- A. 从安全性等级来看，这三个模型安全性从低到高的排序是自主访问控制模型、强 制访问控 制模型和基于角色的访问控制模型

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ B. 自主访问控制是一种广泛应用的方法，资源的所有者（往往也是创建者）可以规定谁有权 访问它们的资源，具有较好的易用性和扩展性

○ C. 强制访问控制模型要求主题和客体都一个固定的安全属性，系统用该安全属性来决定一个 主体是否可以访问某个客体。该模型具有一定的抗恶意程序攻击能力， 适用于专用或安全 性要求较高的系统

○ D. 基于角色的访问控制模型的基本思想是根据用户所担任的角色来决定用户在系统中 的访问权限，该模型便于实施授权管理和安全约束，容易实现最小特权、职责 分离等各种安全策略

回答正确 +1分

15、在信息系统中，访问控制是重要的安全功能之一。他的任务是在用户对系统资源提供最大限 度共享的基础上，对用户的访问权限进行管理，防止对信息的非授权篡改和滥用。 访问控制 模型将实体划分为主体和客体两类，通过对主体身份的识别来限制其对客体的 访问权限。下 列选项中，对主体、客体和访问权限的描述中错误的是（） 分值1分

○ A.对文件进行操作的用户是一种主体

○ B.主体可以接受客体的信息和数据，也可能改变客体相关的信息

○ C.访问权限是指主体对客体所允许的操作

● D.对目录的访问权可分为读、写和拒绝访问

回答正确 +1分

16、小赵是某大学计算机科学与技术专业的毕业生，在前往一家大型企业应聘时，面试经理要求 他给出该企业信息系统访问控模型的设计思路。如果想要为一个存在大量用户的信息系统实 现自主访问控制功能，在以下选项中，从时间和资源消耗的角度，下列选项中他应该采取的 最合适的模型或方法是（） 分值1分

● A. 访问控制列表（ACL）

○ B. 能力表（CL）

○ C. BLP模型

○ D. Biba 模型

回答正确 +1分

17、强制访问控制是指主体和客体都有一个固定的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体，具有较高的安全性。适用于专用或对安全性要求较高的系统， 强制访问 控制模型有多种模型，如BLP、Biba、Clark-Willson 和ChinescWall 等。小李自学了BLP 模型， 并对该模型的特点进行了总结。以下4 种对BLP 模型的描述中，正确的是（） 分值1分

○ A. BLP 模型用于保证系统信息的机密性，规则是“向上读，向下写”

● B. BLP 模型用于保证系统信息的机密性，规则是“向下读，向上写”

○ C. BLP 模型用于保证系统信息的完整性，规则是“向上读，向下写”

○ D. BLP 模型用于保证系统信息的完整性，规则是“向下读，向上写”

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

18、访问控制方法可分为自主访问控制、强制访问控制和基于角色的访问控制，他们具有不同的 特点和应用场景。如果需要选择一个访问控制方法，要求能够支持最小特权原则和 职责分离 原则，而且在不同的系统配置下可以具有不同的安全控制，那么在下列选项 中，能够满足 以上要求的选项是（）。 分值1分

- A. 自主访问控制
- B. 强制访问控制
- C. 基于角色的访问控制
- D. 以上选项都可以

回答正确 +1分

19、关于Wi-Fi 联盟提出的安全协议WPA 和WPA2 的区别，下面描述正确的是（） 分值1分

- A. WPA 是有线局域安全协议，而WPA2 是无线局域网协议
- B. WPA 是适用于中国的无线局域安全协议，而WPA2 适用于全世界的无线局域网协议
- C. WPA 没有使用密码算法对接入进行认证，而WPA2 使用了密码算法对接入进行认证
- D. WPA 是依照802.11i 标准草案制定的，而WPA2 是依照802.11i 正式标准制定的

回答正确 +1分

20、随着高校业务资源逐渐向数据中心高度集中，Web 成为一种普适平台，上面承载了越来越多的核心业务。Web 的开放性带来丰富资源、高效率、新工作方式的同时，也使机构的重要信息 暴露在越来越多的威胁中。去年，某个……网站遭遇SQL 群注入(Mass SQL Injection)攻击，网站发布的重要信息被篡改成为大量签名，所以该校在某信息安全公司的建议下配置了 状态检测防火墙，其原因不包括（） 分值1分

- A. 状态检测防火墙可以应用会话信息决定过滤规则
- B. 状态检测防火墙具有记录通过每个包的详细信息能力
- C. 状态检测防火墙过滤规则与应用层无关，相比于包过滤防火墙更易安装和使用
- D. 状态检测防火墙结合网络配置和安全规定做出接纳、拒绝、身份认证或报警等处理动作答

回答正确 +1分

21、异常入侵检测是入侵检测系统常用的一种技术，它是识别系统或用户的非正常行为或者对于计算机资源的非正常使用，从而检测出入侵行为。下面说法错误的是（） 分值1分

- A. 在异常入侵检测中，观察到的不是已知的入侵行为，而是系统运行过程中的异常现象
- B. 实施异常入侵检测，是将当前获取行为数据和已知入侵攻击行为特征相比较，若匹配则认为 有攻击发生

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ C. 异常入侵检测可以通过获得的网络运行状态数据，判断其中是否含有攻击的企图，并通过多种手段向管理员报警

○ D. 异常入侵检测不但可以发现从外部的攻击，也可以发现内部的恶意行为

回答正确 +1分

22、某集团公司的计算机网络中心内具有公司最重要的设备和信息数据。网络曾在一段时间内依然遭受了几次不小的破坏和干扰,虽然有防火墙,但系统管理人员也未找到真正的事发原因。某网络安全公司为该集团部署基于网络的入侵检测系统(NIDS),将IDS部署在防火墙 后，以进行二次防御。那么 NIDS 不会在()区域部署。 () 分值1分

○ A. DMZ

○ B. 内网主干

○ C. 内网关键子网

● D. 外网入口

回答正确 +1分

23、入侵检测系统有其技术优越性，但也有其局限性，下列说法错误的是（）。 分值1分

● A. 对用户知识要求高、配置、操作和管理使用过于简单，容易遭到攻击

○ B. 入侵检测系统会产生大量的警告消息和可疑的入侵行为记录，用户处理负担很重

○ C. 入侵检测系统在应对自身攻击时，对其他数据的检测可能会被抑制或者受到影响

○ D. 警告消息记录如果不完整，可能无法与入侵行为关联

回答正确 +1分

24、安全域是由一组具有相同安全保护需求并相互信任的系统组成的逻辑区域，下面哪项描述是错误的（）。 分值1分

● A. 安全域划分主要以业务需求、功能需求和安全需求为依据，和网络、设备的物理 部署位置 无关

○ B. 安全域划分能把一个大规模复杂系统的安全问题，化解为更小区域的安全保护问 题

○ C. 以安全域为基础，可以确定该区域的信息系统安全保护等级和防护手段，从而使 同一安全 域内的资产实施统一的保护

○ D. 安全域边界是安全事件发生时的抑制点，以安全域为基础，可以对网络和系统进行安全检 查和评估，因此安全域划分和保护也是网络防攻击的有效防护方式

回答正确 +1分

25、小王是某通信运营商公司的网络按武安架构师，为该公司推出的一项新型通信系统项目做安 全架构规划，项目客户要求对他们的大型电子商务网络进行安全域的划分，化解为小区域的 安全保护，每个逻辑区域有各自的安全访问控制和边界控制策略，以实现大规模电子商务系 统的信息保护。小王对信息系统安全域(保护对象)的划分不需要考虑的是（） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

- A. 业务系统逻辑和应用关联性，业务系统是否需要对外连接
- B. 安全要求的相似性，可用性、保密性和完整性的要求是否类似
- C. 现有网络结构的状况，包括现有网路、地域和机房等
- D. 数据库的安全维护

回答正确 +1分

26、在Windos7 中，通过控制面板（管理工具——本地安全策略——安全设置——账户策略）可以进入操作系统的密码策略设置界面，下面哪项内容不能在该界面进行设置（） 分值1分

- A. 密码必须符合复杂性要求
- B. 密码长度最小值
- C. 强制密码历史
- D. 账号锁定时间

回答正确 +1分

27、Linux 系统中常用数字来表示文件的访问权限，假设某文件的访问限制使用了755来表示，则下面哪项是正确的（） 分值1分

- A. 这个文件可以被任何用户读和写
- B. 这个可以被任何用户读和执行
- C. 这个文件可以被任何用户写和执行
- D. 这个文件不可以被所有用户写和执行

回答正确 +1分

28、操作系统用于管理计算机资源，控制整个系统运行，是计算机软件的基础。操作系统安全是计 算、网络及信息系统安全的基础。一般操作系统都提供了相应的安全配置接口。小王新买了一 台计算机，开机后首先对自带的Windows 操作系统进行配置。他的主要操作有：（1）关闭不 必要的服务和端口；（2）在“在本地安全策略”重配置账号策略、本地策略、公钥策略和IP 安全策略；（3）备份敏感文件，禁止建立空连接，下载最新补丁；（4）关闭审核策略，开启 口令策略，开启账号策略。这些操作中错误的是（） 分值1分

- A. 操作（1），应该关闭不必要的服务和所有端口
- B. 操作（2），在“本地安全策略”中不应该配置公钥策略，而应该配置私钥策略
- C. 操作（3），备份敏感文件会导致这些文件遭到窃取的几率增加
- D. 操作（4），应该开启审核策略

回答正确 +1分

29、在Windows 系统中，存在默认共享功能，方便了局域网用户使用，但对个人用户来说存安全风险。如果电脑联网，网络上的任何人都可以通过共享使用或修改文件。

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

小刘在装有Windows XP 系统的计算机上进行安全设置时，需要关闭默认共享。下列选项中，能关闭默认共享的操作是（） 分值1分

- A. 将"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lenmanserver\paraneters"
- 项中的“Autodisconnect"项键值改为0
- B. 将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lenmanserver\ paraneters"项中的"AutoShareServer"项键值改为0
- C. 将“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services \lenmanserver\paraneters"项中的"AutoShareWks"项键值改为0
- D. 在命令窗口中输入命令，删除C盘默认共享：net share C /del

回答正确 +1分

30、从Linux 内核2.1 版开始，实现了基于权能的特权管理机制，实现了超级用户的特权分割，打破了 UNIX/LINUX 操作系统中超级用户/普通用户的概念，提高了操作系统的安全性。下列 选项中，对特权管理机制的理解错误的是（） 分值1分

- A. 普通用户及其 shell 没有任何权能，而超级用户及其 shell 在系统启动之初拥 有全部 权能
- B. 系统管理员可以剥夺和恢复超级用户的某些权能
- C. 进程可以放弃自己的某些权能
- D. 当普通用户的某些操作涉及特权操作时，仍然通过setuid 实现

回答正确 +1分

31、关于数据库恢复技术，下列说法不正确的是： （） 分值1分

- A. 数据库恢复技术的实现主要依靠各种数据的冗余和恢复机制技术来解决，当数据 库中数据被破坏时，可以利用冗余数据来进行修复
- B. 数据库管理员定期地将整个数据库或部分数据库文件备份到磁带或另一个磁盘上保存起来，是数据库恢复中采用的基本技术
- C. 日志文件在数据库恢复中起着非常重要的作用，可以用来进行事物故障恢复和系统故障恢 复，并协助后备副本进行介质故障恢复
- D. 计算机系统发生故障导致数据未存储到固定存储器上，利用日志文件中故障发生前 数据 的值，将数据库恢复到故障发生前的完整状态，这一对事务的操作称为提交

回答正确 +1分

32、关系数据库的完整性规则是数据库设计的重要内容，下面关于“实体完整性”的描述正确的（） 分值1分

- A. 指数据表中列的完整性，主要用于保证操作的数据(记录)完整、不丢项
- B. 指数据表中行的完整性，主要用于保证操作的数据(记录)非空、唯一且不重复
- C. 指数据表中列必须满足某种特定的数据类型或约束，比如取值范围、数值精度等约束
- D. 指数据表中行必须满足某种特定的数据姓雷或约束，比如在更新、插入或删除记录时，更将关联

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

有关的记录一并处理才可以

回答正确 +1分

33、数据在进行传输前，需要由协议自上而下对数据进行封装。TCP/IP 协议中，数据封装的顺序是：（） 分值1分

- A. 传输层、网络接口层、互联网络层
- B. 传输层、互联网络层、网路接口层
- C. 互联网络层、传输层、网络接口层
- D. 互联网络层、网络接口层、传输层

回答正确 +1分

34、安全多用途互联网邮件扩展（Secure Nultipurpose Internet Mail Pxtension,S/MIME）是（）
指一种保障邮件安全的技术，下面描述错误的是（C） 分值1分

- A. S/MIME采用了非对称密码学机制
- B. S/MIME支持数字证书
- C. S/MIME采用了邮件防火墙技术
- D. S/MIME 支持用户身份认证和邮件加密

回答正确 +1分

35、Apache HTTP Server （简称Apache）是一个开放源码的Web 服务运行平台，在使用过程中，该软件默认会将自己的软件名和版本号发送给客户端。从安全角度出发，为隐藏这些信息，应当采取以下哪种措施（） 分值1分

- A. 不选择Windows平台，应选择在Linux 平台下安装使用
- B. 安装后，修改配置文件http.conf 中的有关参数
- C. 安装后，删除Apsche HTTP Server 源码
- D. 从正确的官方网站下载Apeche HTTP Server，并安装使用

回答正确 +1分

36、Internet Explorer，简称IE,是微软推出的一款Web 浏览器，IE 中有很多安全设置选项，用来设置安全上网环境和保护用户隐私数据。以下哪项不是IE 中的安全配置项目（） 分值1分

- A. 设置Cookie安全，允许用户根据自己安全策略要求者、设置Cookie策略，包括从阻止所有Cookie到接受所有Cookie，用户也可以选择删除已经保存过的Cookie
- B. 禁用自动完成和密码记忆功能，通过设置禁止IE 自动记忆用户输入过的Web地址和表单， 也禁止IE自动记忆表单中的用户名和口令信息
- C. 设置每个连接的最大请求数，修改MuKeepA;ivEcquests，如果同时请求数达到阈值就 不再响应新的请求，从而保证了系统资源不会被某个链接大量占用

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ D. 为网站设置适当的浏览器安全级别，用户可以将各个不同的网站划分到Internet、 本
○ 地Internet、受信任的站点、受限制的站点等不同安全区域中，以采取不同的安全访问策略

回答正确 +1分

37、下面对“零日（zero-day）漏洞”的理解中，正确的是（） 分值1分

○ A. 指一个特定的漏洞，该漏洞每年1月1日零点发作，可以被攻击者用来远程攻击，获取主机权限
○ B. 指一个特定的漏洞，特指在2010 年被发现出来的一种漏洞，该漏洞被“震网” 病毒所利 用，用来攻击伊朗布什尔核电站基础设施
○ C. 指一类漏洞，即特别好被被利用，一旦成功利用该漏洞，可以在1 天内完成攻击，且成功达到攻击目标
● D. 指一类漏洞，即刚被发现后立即被恶意利用的安全漏洞。一般来说，那些已经被小部分人发 现，但是还未公布、还不存在安全补丁的漏洞都是零日漏洞

回答正确 +1分

38、为达到预期的攻击目的，恶意代码通常会被采用各种方法将自己隐藏起来。关于隐藏方法，下面理解错误的是（） 分值1分

○ A. 隐藏恶意代码进程，即将恶意代码进程隐藏起来，或者改名和使用系统进程名， 以更好的 躲避检测，迷惑用户和安全检测人员
○ B. 隐藏恶意代码的网络行为，复用通用的网络端口，以躲避网络行为检测和网络监 控
● C. 隐藏恶意代码的源代码，删除或加密源代码，仅留下加密后的二进制代码，以躲 避用户和 安全检测人员
○ D. 隐藏恶意代码的文件，通过隐藏文件、采用流文件技术或HOOK技术、以躲避系统文件检查和清除

回答正确 +1分

39、某网站管理员小邓在流量监测中发现近期网站的入站ICMP 流量上升250%尽管网站没有发现任何的性能下降或其他问题，但为了安全起见，他仍然向主管领导提出了应对措施，作为主管负责人，请选择有效的针对此问题的应对措施： () 分值1分

● A. 在防火墙上设置策略，阻止所有的ICMP 流量进入(关掉ping)
○ B. 删除服务器上的ping.exe 程序
○ C. 增加带宽以应对可能的拒绝服务攻击
○ D. 增加网站服务以应对即将来临的拒绝服务攻击

回答正确 +1分

40、下面四款安全测试软件中，主要用于WEB 安全色扫描的是（） 分值1分

○ A. Cisco Auditing Tools
● B. Acunetix Web Vulnerability Scanner

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ C. NMAP

○ D. ISS Database Scanner

回答正确 +1分

41、关于ARP 欺骗原理和防范措施，下面理解错误的是（） 分值1分

○ A. ARP欺骗是指攻击者直接向受害者主机发送错误的ARP 应答报文，使得受害者主机将错误的硬件地址映射关系存入到ARP缓存中，从而起到冒充主机的目的

○ B. 单纯利用ARP 欺骗攻击时，ARP欺骗通常影响的是内部子网，不能跨越路由实施攻击

○ C. 解决ARP欺骗的一个有效方法是采用“静态”的ARP缓存，如果发生硬件地址的更改，则需要人工更新缓存

● D. 彻底解决ARP 欺骗的方法是避免使用ARP 协议和ARP 缓存，直接采用IP 地址和其他主机进 行连接

回答正确 +1分

42、在软件保障成熟度模型(Software Assurance Maturity Mode，SAMM)中规定了软件开发过
程中的核心业务功能，下列哪个选项不属于核心业务功能： （） 分值1分

○ A. 治理，主要是管理软件开发的过程和活动

○ B. 构造，主要是在开发项目中确定目标并开发软件的过程与活动

○ C. 验证，主要是测试和验证软件的过程与活动

● D. 购置，主要是购买第三方商业软件或者采用开源组件的相关管理过程与活动

回答正确 +1分

43、针对软件的拒绝服务攻击时通过消耗系统资源是软件无法响应正常请求的一种攻击方式， 在软件开发时分析拒绝服务攻击的威胁，以下哪个不是需要考虑的攻击方式（） 分值1分

○ A. 攻击者利用软件存在逻辑错误，通过发送某种类型数据导致运算进入死循环，CPU资源占用始终100%

○ B. 攻击者利用软件脚本使用多重账套查询在数据量大时会导致查询效率低，通过发送大 量的 查询导致数据库相应缓慢

○ C. 攻击者利用软件不自动释放连接的问题，通过发送大量连接的消耗软件并发生连接数，导 致并发连接数耗尽而无法访问

● D. 攻击者买通了IDC 人员，将某软件运行服务器的网线拔掉导致无法访问

回答正确 +1分

44、某网站为了更好向用户提供服务，在新版本设计时提供了用户快捷登陆功能，用户如果使用上次的IP地址进行访问，就可以无需验证直接登录，该功能推出后，导致大量用户账号被盗用，关于以上问题的说法正确的是： （） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ A. 网站问题是由于开发人员不熟悉安全编码，编写了不安全的代码导致攻击面增大，产生此安全问题

○ B. 网站问题是由于用户缺乏安全意识导致，使用了不安全的功能，导致网站攻击面增大，产生 此问题

○ C. 网站问题是由于使用便利性提高带来网站用户数增加，导致网络攻击面增大，产生此安全问题

● D. 网站问题是设计人员不了解安全设计关键要素，设计了不安全的功能，导致网站攻击面增大，产生此安全问题

回答正确 +1分

45、下面有关软件安全问题的描述中，哪项不是由于软件设计缺陷引起的（）
分值1分

● A. 设计了用户权限分级机制和最小特权原则，导致软件在发布运行后，系统管理员 不能查看系统审计信息

○ B. 设计了采用不加盐(SALT)的SHA-1算法对用户口令进行加密存储，导致软件在发布运 行后，不同的用户如使用了相同的口令会得到相同的加密结果，从而可以假冒其他用户登录

○ C. 设计了缓存用户隐私数据机制以加快系统处理性能，导致软件在发布运行后，被黑客攻击获取到用户隐私数据

○ D. 设计了采用自行设计的加密算法对网络传输数据进行保护，导致软件在发布运行 后，被攻击对手截获网络数据并破解后得到明文

回答正确 +1分

46、某购物网站开发项目经过需求分析进入系统设计阶段，为了保证用户账户的安全，项目开发人员决定用户登录时如用户名或口令输入错误，给用户返回“用户名或口令输入错误”信息，输入错误达到三次，将暂时禁止登录该账户，请问以上安全设计遵循的是哪项安全设计原则： （） 分值1分

○ A. 最小共享机制原则

○ B. 经济机制原则

● C. 不信任原则

○ D. 默认故障处理保护原则

回答正确 +1分

47、为了保障系统安全，某单位需要对其跨地区大型网络实时应用系统进行渗透测试，以下关于渗透测试过程的说法不正确的是： （） 分值1分

○ A. 由于在实际渗透测试过程中存在不可预知的风险，所以测试前要提醒用户进行系 统和数据备份，以便出现问题时可以及时恢复系统和数据

○ B. 渗透测试从“逆向”的角度出发，测试软件系统的安全性，其价值在于可以测试软件在实 际系统中运行时的安全状况

○ C. 渗透测试应当经过方案制定、信息收集、漏洞利用、完成渗透测试报告等步骤

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● D. 为了深入发掘该系统存在的安全威胁应该在系统正常业务运行高峰期进行渗透测试

回答正确 +1分

48、小王在学习信息安全管理体系相关知识之后，对于建立信息安全管理体系，自己总结了下面四条要求，其中理解不正确的是（） 分值1分

○ A. 信息安全管理体系的建立应参照国际国内有关标准实施，因为这些标准是标准化组织在总结研究了很多实际的或潜在的问题后，制定的能共同的和重复使用的规则

● B. 信息安全管理体系的建立应基于最新的信息安全技术，因为这是国家有关信息安 全的法律 和法规方面的要求，这体现以预防控制为主的思想

○ C. 信息安全管理体系应强调全过程和动态控制的思想，因为安全问题是动态的，系统所处的安全环境也不会一成不变的，不可能建设永远安全的系统

○ D. 信息安全管理体系应体现科学性和全面性的特点，因为要对信息安全管理设计的方方面面实施较为均衡的管理，避免遗漏某些方面而导致组织的整体信息安全水平过低

回答正确 +1分

49、美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)隶属美国商务部，NIST 发布的很多关于计算机安全的指南文档。下面哪 个文档是由NIST 发布的（） 分值1分

○ A. ISO 27001〈〈Information technology —Security techniques —Informtion security management systems-Requirements》

○ B. X.509〈〈Information Technology —Open Systems —The Directory:Authentication Framcwork》

● C. SP 800-37《Guide for Applying the Risk Management Framcwork to Federal Information Systems》

○ D. RFC 2402 《IP Authenticat Header》

回答正确 +1分

50、小牛在对某公司的信息系统进行风险评估后，因考虑到该业务系统中部分涉及金融交易的功能模块风险太高，他建议该公司以放弃这个功能模块的方式来处理该风险。请问这种风险处 置的方法是（） 分值1分

○ A. 降低风险

● B. 规避风险

○ C. 转移风险

○ D. 放弃风险

回答正确 +1分

51、残余风险是风险管理中的一个重要概念。在信息安全风险管理中，关于残余风险描述错误的是（） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ A. 残余风险是采取了安全措施后，仍然可能存在的风险：一般来说，是在综合考虑 了安全成本与效益后不去控制的风险

○ B. 残余风险应受到密切监视，它会随着时间的推移而发生变化，可能会在将来诱发 新的安全事件

○ C. 实施风险处理时，应将残余风险清单告知信息系统所在组织的高管，使其了解残余风险的存在和可能造成的后果

● D. 信息安全风险处理的主要准则是尽可能降低和控制信息安全风险，以最小残余风 险值作为 风险管理效果评估指标

回答正确 +1分

52、在信息安全管理过程中，背景建立是实施工作的第一步。下面哪项理解是错误的（）。 分值1分

○ A. 背景建立的依据是国家、地区或行业的相关政策、法律、法规和标准，以及机构的使命、 信息系统的业务目标和特性

● B. 背景建立阶段应识别需要保护的资产、面临的威胁以及存在的脆弱性并分别赋 值，同时确 认已有的安全措施，形成需要保护的资产清单

○ C. 背景建立阶段应调查信息系统的业务目标、业务特性、管理特性和技术特性，形成信息系统的描述报告

○ D. 背景建立阶段应分析信息系统的体系结构和关键要素，分析信息系统的安全环境和要求，形成信息系统的安全要求报告

回答正确 +1分

53、降低风险(或减低风险)是指通过对面临风险的资产采取保护措施的方式来降低风险，下面哪个措施不属于降低风险的措施（） 分值1分

○ A. 减少威胁源。采用法律的手段制按计算机犯罪，发挥法律的威慑作用，从而有效遏制威胁源的动机

● B. 签订外包服务合同。将有技术难点、存在实现风险的任务通过签订外部合同的方 式交予第 三方公司完成，通过合同责任条款来应对风险

○ C. 减少脆弱性。及时给系统补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性

回答正确 +1分

54、某单位在一次信息安全风险管理活动中，风险评估报告提出服务器A 的FTP 服务存在高风险漏洞。随后该单位在风险处理时选择了关闭FTP 服务的处理措施。请问该措施属于哪种 风险处理方式（） 分值1分

○ A. 风险降低

● B. 风险规避

○ C. 风险转移

○ D. 风险接受

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

55、小李在某单位是负责信息安全风险管理方面工作的部门领导，主要负责对所在行业的新人进行基本业务素质培训，一次培训的时候，小李主要负责讲解风险评估方法。请问小李的所述论点中错误的是哪项：（） 分值1分

- A. 风险评估方法包括：定性风险分析、定量风险分析以及半定量风险分析
- B. 定性风险分析需要凭借分析者的经验和直觉或者业界的标准和惯例，因此具有随意性
- C. 定量风险分析试图在计算风险评估与成本效益分析期间收集的各个组成部分的具体数字值因此更具有客观性
- D. 半定量风险分析技术主要指在风险分析过程中综合使用定性和定量风险分析技术对风险要素的赋值方式，实现对风险各要素的度量数值化

回答正确 +1分

56、信息安全风险评估是信息安全风险管理工作中的重要环节。在国家网络与信息安全协调 小组 发布的《关于开展信息安全风险评估工作的意见》(国信办[2006]5 号)中，风险评估分为 自评估和检查评估两种形式，并对两种工作形势提出了有关工作原则和要求。 下面选项中描 述正确的是（） 分值1分

- A. 信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充
- B. 信息安全风险评估应以检查评估为主，自评估和检查评估相互结合、互为补充
- C. 自评估和检查评估时相互排斥的，单位应慎重地从两种工作形式选择一个，并长期使用
- D. 自评估和检查评估是相互排斥的，无特殊理由的单位均应选择检查评估，以保证安全效果

回答正确 +1分

57、信息安全风险评估是信息安全风险管理工作中的重要环节。在〈关于开展信息安全风险评估工作的意见》(国信办[2006]5 号)中，指出了风险评估分为自评估和检查评估两种形式，并对两种工作形式提出了有关工作原则和要求。下面选项中描述错误的是（） 分值1分

- A. 自评估是由信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估
- B. 检查评估是指信息系统上级管理部门组织的国家有关职能部门依法开展的风险评估
- C. 信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充
- D. 自评估和检查评估是相互排斥的，单位应慎重地从两种工作形式选择一个，并坚持

回答正确 +1分

58、王工是某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，发现当前案例中共有两个重要资产：资产A1 和资产A2;其中资产A1 面临两个主要威胁，威胁T1 和威胁T2;而资产A2 面临一个主要威胁，威胁T3;威胁T1 可以利用的资产A1 存在的两个脆弱性；脆弱性VI 和脆弱性V2;威胁T2可以利用的资产A1 存在的三个 脆弱性，脆弱性V3、脆弱性V4 和脆弱性V5;威胁T3 可以利用的资产A2 存在的两个脆 弱性；脆弱性V6 和脆弱性V7•根据上述条件，请问：使用相乘法时，应该为资产A1 计

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

算几个风险值（） 分值1分

○ A. 2

○ B. 3

● C. 5

○ D. 6

回答正确 +1分

59、在信息安全管理体系的实施过程中，管理者的作用对于信息安全管理体系能否成功实施非常重要，但是以下选项中不属于管理者应有职责的是（） 分值1分

○ A. 制定并颁布信息安全方针，为组织的信息安全管理体系建设指明方向并提供总体 纲领，明 确总体要求

○ B. 确保组织的信息安全管理体系目标和相应的计划得以制定，目标应明确、可度 量，计划应 具体、可实施

○ C. 向组织传达满足信息安全的重要性，传达满足信息安全要求、达成信息安全目 标、符合信 息安全方针、履行法律责任和持续改进的重要性

● D. 建立健全信息安全制度，明确安全风险管理作用，实施信息安全风险评估过程， 确保信息 安全风险评估技术选择合理、计算正确

回答正确 +1分

60、信息安全管理体系(Information Security Management System，ISMS)的内部审核和管理
审核是两项重要的管理活动。关于这两者，下面描述错误的是（） 分值1分

○ A. 内部审核和管理审评都很重要，都是促进ISMS持续改进的重要动力，也都应当按照一定的周期实施

○ B. 内部审核的实施方式多采用文件审核和现场审核的形式，而管理评审的实施方式多采用召开管理审评会议的形式进行

● C. 内部审核的实施主体由组织内部的ISMS 内审小组，而管理评审的实施主体是由国家政策 指定的第三方技术服务机构

○ D. 组织的信息安全方针、信息安全目标和有关ISMS 文件等，在内部审核中作为审核准使用，但在管理评审中，这些文件是被审对象

回答正确 +1分

61、随着信息安全涉及的范围越来越广，各个组织对信息安全管理的需求越来越迫切，越来越多的组织开始尝试使用参考ISO27001 介绍的ISMS 来实施信息安全管理体系，提高组织的信息安全管理能力。关于ISMS，下面描述错误的是（） 分值1分

● A. 在组织中，应有信息技术责任部门(如信息中心)制定并颁布信息安全方针，为组织的ISMS建设指明方向并提供总体纲领，明确总体要求

○ B. 组织的管理层应确保ISMS 目标和相应的计划得以制定，信息安全管理目标应明确、可度量， 风

险管理计划应具体、具备可行性

○ C. 组织的信息安全目标、信息安全方针和要求应传达到全组织范围内，应包括全体员工，同时也应传达客户、合作伙伴和供应商等外部各方

○ D. 组织的管理层应全面了解组织所面临的信息安全风险，决定风险可接受级别和风险可接受准则，并确认接受和相关残余风险

回答正确 +1分

62、在风险管理中，残余风险是指在实施了新的或增强的安全措施后还剩下的风险，关于残余风险，下面描述错误的是（） 分值1分

○ A. 风险处理措施确定以后，应编制详细的残余风险清单，并获得管理层对残余风险的书面批准，这也是风险管理中的一个重要过程

○ B. 管理层确认接受残余风险，是对风险评估工作的一种肯定，表示管理层已经全面了解了组织所面临的风险，并理解在风险一旦变为现实后，组织能够且必须承担 引发的后果

○ C. 接受残余风险，则表明没有必要防范和加固所有的安全漏洞，也没有必要无限制地提高安 全保护措施的强度，对安全保护措施的选择要考虑到成本和技术的等因 素的限制

● D. 如果残余风险没有降低到可接受的级别，则只能被动地选择接受风险，即对风险 不采取进 一步的处理措施，接受风险可能带来的结果

回答正确 +1分

63、GB/T 22080-2008 《信息技术安全技术 信息安全管理体系 要求》指出，建立信息安全管理体系应参照PDCA 模型进行，即信息安全谷那里体系应包括建立ISMS、实施和运行ISMS、监视和评审ISMS、保持和改进ISMS 等过程，并在这些过程中应实施若干活动。请选出以下描述错误的选项（） 分值1分

○ A. “制定ISMS方针”是建立ISMS阶段工作内容

○ B. “实施培训和意识教育计划”是实施和运行ISMS阶段工作内容

○ C. “进行有效性测量”是监视和评审ISMS阶段工作内容

● D. “实施内部审核”是保持和改进ISMS 阶段工作内容

回答正确 +1分

64、若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T 22080标准要求，其信息安全控制措施通常在以下方面实施常规控制，不包括哪一项（） 分值1分

○ A. 信息安全方针、信息安全组织、资产管理

○ B. 人力资源安全、物力和环境安全、通信和操作管理

○ C. 访问控制、信息系统获取、开发和维护、符合性

● D. 规划与建立ISMS

回答正确 +1分

65、信息安全组织的管理涉及内部组织和外部各方面两个控制目标，为了实现对组织

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

内部信息安全的有效管理，应该实施常规的控制措施，不包括哪些选项（） 分值1分

- A. 信息安全的管理承诺、信息安全协调、信息安全职责的分配
- B. 信息处理设施的授权过程、保密性协议、与政府部门的联系
- C. 与特定利益集团的联系、信息安全的独立评审
- D. 与外部各方相关风险的识别、处理外部各方协议中的安全问题

回答正确 +1分

66、若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T 22080标准要求，其信息安全措施通常需要在资产管理方面实施常规控制，资产管理包含对资产负责和信息分类两个控制目标。信息分类控制的目标是为了确保信息受到适当级别的保护，通常采取以下 哪项控制 措施（） 分值1分

- A. 资产清单
- B. 资产责任人
- C. 资产的可接受使用
- D. 分类指南、信息的标记和处理

回答正确 +1分

67、应急响应时信息安全事件管理的重要内容之一。关于应急响应工作，下面描述错误的是（） 分值1分

- A. 信息安全应急响应，通常是指一个组织为了应对各种安全意外事件的发生所采取的防范措施，既包括预防性措施，也包括事业发生后的应对措施
- B. 应急响应工作有其鲜明的特点：具体高技术复杂性与专业性、强突发性、对知识经验的高依赖性，以及需要广泛的协调与合作
- C. 应急响应时组织在处置应对突发/重大信息安全事件时的工作，其主要包括两部 分工作： 安全事件发生时正确指挥、事件发生后全面总结
- D. 应急响应工作的起源和相关机构的成立和1988 年11 月发生的莫里斯蠕虫病毒事件有关， 基于该事件，人们更加重视安全事件的应急处理和整体协调的重要性

回答正确 +1分

68、我国依照信息系统的重要程度、安全事件造成的系统损失以及带来的社会影响等因素，将信息安全事件分为若干个级别，其中，能够对特别重要的信息系统产生特别严重影响或破坏的信息安全事件，如使特别重要信息系统遭受特别重大的系统损失，如造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到 严重破坏的，应属 于哪一级信息安全事件（） 分值1分

- A. I 级
- B. 皿级
- C. W 级
- D. 特别级

回答正确 +1分

69、恢复时间目标(Recovery Time Objective,RTO)和恢复点目标(RECOVERY PointObjective,RPO)是业务连续性和灾难恢复工作中的两个重要指标，随着信息系统越来越重要和信息技术越来越先进，这两个指标的数值越来越小。小华准备为其工作的信息系 统拟定RTO 和RPO 指标，则以下描述中，正确的是（） 分值1分

- A. RTO 可以为0，RPO 也可以为0
- B. RTO可以为0，RPO不可以为0
- C. RTO不可以为0，RPO可以为0
- D. RTO不可以为0，RPO也不可以为0

回答正确 +1分

70、随着信息技术的不断发展，信息系统的重要性也越来越突出，而与此同时，发生的信息安全事件也越来越多。综合分析信息安全问题产生的根源，下面描述正确的是（） 分值1分

- A. 信息系统自身存在脆弱性是根本原因。信息系统越来越重要，同时自身在开发、部署和使用过程中存在的脆弱性，导致了诸多的信息安全事件发生。因此，杜绝脆弱性的存在是解决信息安全问题的根本所在
- B. 信息系统面临诸多黑客的威胁，包括恶意攻击者和恶作剧攻击者。信息系统应用越来越广泛，接触信息系统的人越多，信息系统越可能遭受攻击。因此，避免有恶意攻击可能的人接触信息系统就可以解决信息安全问题
- C. 信息安全问题产生的根源要从内因和外因两个方面分析，因为信息系统自身存在脆弱性，同时外部又有威胁源，从而导致信息系统可能发生安全事件。因此，要防范信息安全风险，需从内外因同时着手
- D. 信息安全问题的根本原因是内因、外因和人三个因素的综合作用，内因和外因都可能导致安全事件的发生，但最重要的还是人的因素，外部攻击者和内部工作人 员通过远程攻击、本地 破坏和内外勾结等手段导致安全事件发生。因此，对人这 个因素的防范应是安全工作重点

回答正确 +1分

71、关于信息安全保障技术框架(Information Assurance Tehnical Framework,IATF)，下面描
述错误的是（） 分值1分

- A. IATF 最初由美国国家安全局(NSA)发布，后来由国际标准化组织(ISO)转化为国际标准，供各个国家信息系统建设参考使用
- B. IATF 是一个通用框架，可以用到多种应用场景中，通过对复杂信息系统进行解构和描述， 然后再以此框架讨论信息系统的安全保护问题
- C. IATF 提出了深度防御的战略思想，并提供一个框架进行多层保护，以此防范信息系统面临的各种威胁

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ D. 强调人、技术和操作是深度防御的三个主要层面，也就是说讨论人在技术支持下运行维护的信息安全保障问题

回答正确 +1分

72、关于信息安全保障技术框架（IATF）,以下说法不正确的是：（） 分值1分

○ A. 分层策略允许在适当的时候采用低安全级保障解决方案以便降低信息安全保障的成本

○ B. IATF 从人、技术和操作三个层面提供一个框架实施多层保护，使攻击者即使攻 破一层也无法破坏整个信息基础设施

○ C. 允许在关键区域（例如区域边界）使用高安全级保障解决方案，确保系统安全性

● D. IATF 深度防御战略要求在网络体系结构的各个可能位置实现所有信息安全保障机制

回答正确 +1分

73、2003 年以来，我国高度重视信息安全保障工作，先后制定并发布了多个文件，从政策层面为开展并推进信息安全保障工作进行了规划。下面选项中哪个不是我国发布的文件（） 分值1分

○ A.《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

● B.《国家网络安全综合计划（CNCI）》（国令[2008]54 号）

○ C.《国家信息安全战略报告》（国信[2005]2 号）

○ D.《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23 号）

回答正确 +1分

74、在信息安全保障工作中，人才是非常重要的因素，近年来，我国一直高度重视我国信息安全人才队伍的培养和建设。在以下关于我国关于人才培养工作的描述中，错误的是（） 分值1分

○ A. 在《国家信息化领导小组关于加强信息安全保障工作的意见》仲办发[2003]27 号）中，针对信息安全人才建设与培养工作提出了“加快新鲜全人才培养，增强全民信息安全意识”的指导精神

○ B. 2015 年，为加快网络空间安全高层次人才培养，经报国务院学位委员会批准，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，这对于我国网络信息安全人才成体系化、规模化、系统化培养起到积极的推动作用

● C. 经过十余年的发展，我国信息安全人才培养已经成熟和体系化，每年培养的信息安全从业人员的数量较多，基本能同社会实际需求相匹配；同时，高校信息安全专业毕业人才的综合能力 要求高、知识更全面，因而社会化培养应重点放在非安全专业人才培养上

○ D. 除正规大学教育外，我国信息安全人才非学历教育已基本形成了以各种认证为核心，辅以各种职业技能培训的信息安全人才培训体系，包括“注册信息安全专业人员（CISP）”资质认证和一些大型企业的信息安全资质认证

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

75、2008 年1 月2 日，美国发布第54 号总统令，建立国家网络安全综合计划（ComprehensiveNational Cybersecuity Initative,CNCI ）。CNCI 计划建立三道防 线：第一道防线，减少漏洞和隐患，预防入侵；第二道防线，全面应对各类威胁；第三道防线，强化未来安全环境。从以上内容，我们可以看出以下哪种分析是正确的： ()
分值1分

- ● A. CNCI是以风险为核心，三道防线首要的任务是降低其网络所面临的风险
- ○ B. 从CNCI 可以看出，威胁主要是来自外部的，而漏洞和隐患主要是存在于内部的
- ○ C. CNCI 的目的是尽快研发并部署新技术和彻底改变其糟糕的网络安全现状，而不是在现在的网络基础上修修补补
- ○ D. CNCI 彻底改变了以往的美国信息安全战略，不再把关键基础设施视为信息安全保障重点，而是追求所有网络和系统的全面安全保障

回答正确 +1分

76、公司甲做了很多政府网站安全项目，在为网游公司乙的网站设计安全保障方案时，借鉴以前项目经验，为乙设计了多重数据加密安全措施，但用户提出不需要这些加密措施，理由是影 响了网站性能，使用户访问量受限。双方引起争议。下面说法哪个是错误的： () 分值1分

- ● A. 乙对信息安全不重视，低估了黑客能力，不舍得花钱
- ○ B. 甲在需求分析阶段没有进行风险评估，所部属的加密针对性不足，造成浪费
- ○ C. 甲未充分考虑网游网站的业务与政府网站业务的区别
- ○ D. 乙要综合考虑业务、合规性和风险，与甲共同确定网站安全需求

回答正确 +1分

77、为保障信息系统的安全，某经营公共服务系统的公司准备并编制一份针对性的信息安全保障方案，并将编制任务交给了小王，为此，小王决定首先编制出一份信息安全需求报告。关于此项工作，下面说法错误的是（） 分值1分

- ○ A. 信息安全需求是安全方案设计和安全措施的依据
- ○ B. 信息安全需求应当是从信息系统所有者(用户)的角度出发，使用规范化、结构化的语言来描述信息系统安全保障需求
- ○ C. 信息安全需求应当基于信息安全风险评估结果、业务需求和有关政策法规和标准的合规性要求得到
- ● D. 信息安全需求来自于该公众服务信息系统的功能设计方案

回答正确 +1分

78、从系统工程的角度来处理信息安全问题，以下说法错误的是： () 分值1分

- ○ A. 系统安全工程旨在了解企业存在的安全风险，建立一组平衡的安全需求，融合各种工程学科的努力将此安全需求转换为贯穿系统整个生存期的工程实施指南
- ○ B. 系统安全工程需对安全机制的正确性和有效性做出诠释，证明安全系统的信任度能够达到企业的

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

要求，或系统遗留的安全薄弱性在可容许范围之内

● C. 系统安全工程能力成熟度模型(SSE-CMM)是一种衡量安全工程实践能力的方法，是一种使用面向开发的方法

○ D. 系统安全工程能力成熟度模型(SSE-CMM)是在原有能力成熟度模型(CMM)的基础上。通过对安全工作过程进行管理的途径，将系统安全工程转变为一个完好定义的、成熟的、可测量的先进学科

回答正确 +1分

79、某项目的主要内容为建造A类机房，监理单位需要根据《电子信息系统机房设计规范》(GB50174-2008)的相关要求，对承建单位的施工设计方案进行审核，以下关于监理单 位给出的审核意见错误的是（） 分值1分

○ A. 在异地建立备份机房，设计时应与主要机房等级相同

○ B. 由于高端小型机发热量大，因此采用活动地板下送风，上回风的方式

○ C. 因机房属于A 级主机房，因此设计方案中应考虑配备柴油发电机，当市电发生故障时所配备的柴油发电机应能承担全部负荷的需要

● D. A 级主机房应设置自动喷水灭火系统

回答正确 +1分

80、某公司建设面向内部员工的办公自动化系统和面向外部客户的营销系统，通过公开招标选择M 公司为实施单位，并选择了H监理公司承担该项目的全程监理工作。目前，各个应用系统均已完成开发，M 公司已经提交了验收申请。监理公司需要对M 公司提交的软件配置文件进行审查，在以下所提交的文档中，哪一项属于开发类文档：（） 分值1分

○ A. 项目计划书

○ B. 质量控制计划

○ C. 评审报告

● D. 需求说明书

回答正确 +1分

81、有关系统安全工程-能力成熟度模型(SEE-CMM)中的基本实施(Base Practices，BP)， 正确的理解是： （） 分值1分

● A. BP 不限定于特定的方法或工具，不同的业务背景中可以使用不同的方法

○ B. BP 不是根据广泛的现有资料、实践和专家意见综合得出的

○ C. BP 不代表信息安全工程领域的最佳实践

○ D. BP不是过程区域(Process Areas,PA)的强制项

回答正确 +1分

82、在使用系统安全工程-能力成熟度模型(SSE-CMM)对一个组织的安全工程能力成熟度进行测量时，有关测量结果，错误的理解是： （） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ A. 如果该组织在执行某个特定的过程区域时具备某一个特定级别的部分公共特征时，则这个组织在这个过程区域的能力成熟度未达到此级

● B. 如果该组织某个过程区域(Process Areas,PA)具备了 “定义标准过程”、“执行已定 义的过程”两个公共特征，则过程区域的能力成熟度级别达到3 级 “充分定义级”

○ C. 如果某个过程区域(Process Areas,PA)包含4 个基本实施(Base Practices，BP)，执行此PA时执行了3 个BP，则此过程区域的能力成熟度级别为0

○ D. 组织在不同的过程区域的能力成熟度可能处于不同的级别上

回答正确 +1分

83、从历史演进来看，信息安全的发展经历了多个阶段。其中，有一个阶段的特点是：网络信息系统逐步形成，信息安全注重保护信息在存储、处理和传输过程中免受非授权的访问，开始使用防火墙、防病毒、PKI 和VPN 等安全产品。这个阶段是（） 分值1分

○ A. 通信安全阶段

○ B. 计算机安全阶

● C. 信息系统安全阶段

○ D. 信息安全保障阶段

回答正确 +1分

84、下面关于信息系统安全保障模型的说法不正确的是：（） 分值1分

○ A. 国家标准《信息系统安全保障评估框架第一部分：简介和一般模型》(GB/T20274.1-2006) 中的信息系统安全保障模型将风险和策略作为基础和核心

○ B. 模型中的信息系统生命周期模型是抽象的概念性说明模型，在信息系统安全保障具体操作时， 可根据具体环境和要求进行改动和细化

○ C. 信息系统安全保障强调的是动态持续性的长效安全，而不仅是某时间点下的安全

● D. 信息系统安全保障主要是确保信息系统的保密性、完整性和可用性，单位对信息系统运行维 护和使用的人员在能力和培训方面不需要投入

回答正确 +1分

85、《信息安全保障技术框架》(Information Assurance Technical Framework，IATF)是由哪个下面哪个国家发布的（） 分值1分

○ A 中国

● B. 美国

○ C. 俄罗斯

○ D. 欧盟

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

86、我国信息安全保障工作先后经历了启动、逐步展开和积极推进，以及深化落实三个阶段,我国信息安全保障各阶段说法不正确的是：（） 分值1分

○ A. 2001 年，国家信息化领导小组重组，网络与信息安全协调小组成立，我国信息安全保障 工作正式启动

○ B. 2003 年7 月，国家信息化领导小组制定出台了《关于加强信息安全保障工作的意见》(中办发27号文件)，明确了“积极防御、综合防范”的国家信息安全保障工作方针

● C. 2003 年，中办发 27 号文件的发布标志着我国信息安全保障进入深化落实阶段

○ D. 在深化落实阶段，信息安全法律法规、标准化，信息安全基础设施建设，以及信息安全等级保护和风险评估取得了新进展

回答正确 +1分

87、 我国信息安全保障建设包括信息安全组织与管理体制、基础设施、技术体系等方面，以下关于信息安全保障建设主要工作内容说法不正确的是：（） 分值1分

○ A. 健全国家信息安全组织与管理体制机制，加强信息安全工作的组织保障

○ B. 建设信息安全基础设施，提供国家信息安全保障能力支撑

● C. 建立信息安全技术体系，实现国家信息化发展的自主创新

○ D. 建立信息安全人才培养体系，加快信息安全科学建设和信息安全人才培养

回答正确 +1分

88、某银行信息系统为了满足业务发展的需要准备进行升级改造，以下哪一项不是此次改造中信息系统安全需求分析过程需要考虑的主要因素（） 分值1分

○ A. 信息系统安全必须遵循的相关法律法规，国家以及金融行业安全标

○ B. 信息系统所承载该银行业务正常运行的安全需求

● C. 消除或降低该银行信息系统面临的所有安全风险

○ D. 该银行整体安全策略

回答正确 +1分

89、信息安全测评是指依据相关标准，从安全功能等角度对信息技术产品、信息系统、服务提供商以及人员进行测试和评估，以下关于信息安全测评说法不正确的是：（） 分值1分

○ A. 信息产品安全评估是测评机构对产品的安全性做出的独立评价，增强用户对已评估产品安全的信任

● B. 目前我国常见的信息系统安全测评包括信息系统风险评估和信息系统安全保障测评两种类 型

○ C. 信息安全工程能力评估是对信息安全服务提供者的资格状况、技术实力和实施服务过程质量保证能力的具体衡量和评价

○ D. 信息系统风险评估是系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件可能造成的危害程度，提出有针对性的安全防护策略和整改措施

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

回答正确 +1分

90、美国的关键信息基础设施(Critical InformationInfrastructure，CII)包括商用核设施、政府设
施、交通系统、饮用水和废水处理系统、公共健康和医疗、能源、银行和金融、国防工业基地等等，美国政府强调重点保障这些基础设施信息安全，其主要原因不包括：（） 分值1分

- A. 这些行业都关系到国计民生，对经济运行和国家安全影响深远
- B. 这些行业都是信息化应用广泛的领域
- C. 这些行业信息系统普遍存在安全隐患，而且信息安全专业人士缺乏的现象比其他行业更突出
- D. 这些行业发生信息安全事件，会造成广泛而严重的损失

回答正确 +1分

91、在设计信息系统安全保障方案时，以下哪个做法是错误的：（） 分值1分

- A. 要充分切合信息安全需求并且实际可行
- B. 要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量控制成本
- C. 要充分采取新技术，在使用过程中不断完善成熟，精益求精，实现技术投入保值要求
- D. 要充分考虑用户管理和文化的可接受性，减少系统方案实施障碍

回答正确 +1分

92、部署互联网协议安全虚拟专用网(Internet protocol Security Virtual Private Network， IPsec VPN)时，以下说法正确的是：（） 分值1分

- A. 配置MD5安全算法可以提供可靠地数据加密
- B. 配 置AES 算法可以提供可靠的数据完整性验证
- C. 部署 IPsec VPN 网络时，需要考虑IP 地址的规划，尽量在分支节点使用可以聚合的IP 地址段，来减少IPsec 安全关联(Security Authentication，SA)资源的消耗
- D. 报文验证头协议(Authentication Header，AH)可以提供数据机密性

回答正确 +1分

93、某单位系统管理员对组织内核心资源的访问制定访问策略，针对每个用户指明能够访问 的资源，对于不在指定资源列表中的对象不允许访问。该访问控制策略属于以下哪一种：（） 分值1分

- A. 强制访问控制
- B. 基于角色的访问控制
- C. 自主访问控制
- D. 基于任务的访问控制

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

94、主体和客体是访问控制模型中常用的概念。下面描述种错误的是（） 分值1分

- A. 主体是访问的发起者，是一个主动的实体，可以操作被动实体的相关信息或数据
- B. 客体也是一种实体，是操作的对象，是被规定需要保护的资源
- C. 主体是动作的实施者，比如人、进程或设备等均是主体，这些对象不能被当作客体使用
- D. 一个主体为了完成任务，可以创建另外的主体，这些主体可以独立运行

回答正确 +1分

95、以下场景描述了基于角色的访问控制模型(Role-based Access Control，RBAC):根据组织的
业务要求或管理要求，在业务系统中设置若干岗位、职位或分工。管理员负责将权限(不同类别和级别的) 分别赋予承担不同工作职责的用户。关于RBAC 模型，下列说法错误的 是： （） 分值1分

- A. 当用户请求访问某资源时，如果其操作权限不再用户当前被激活角色的授权范围内，访问请求将被拒绝
- B. 业务系统中的岗位、职位或者分工，可对应RBAC 模型中的角色
- C. 通过角色，可实现对信息资源访问的控制
- D. RBAC 模型不能实现多级安全中的访问控制

回答正确 +1分

96、自主访问控制模型（）的访问控制关系可以用访问控制(ACL)来表示，该ACL 利用在客体上附加一个主体明细表的方法来表示访问控制矩阵，通常使用由客体指向的链表来存储相 关数据。下面选项中说法正确的是(D) 分值1分

- A. ACL是Bell-LaPadula 模型的一种具体实现
- B. ACL 在删除用户时，去除该用户所有的访问权限比较方便
- C. ACL 对于统计某个主体能访问哪些客体比较方便
- D. ACL 在增加客体时，增加相关的访问控制权限较为简单

回答正确 +1分

97、关于Kerberos 认证协议，以下说法错误的是： （） 分值1分

- A. 只要用户拿到了认证服务器(AS)发送的票据许可票据(TGT)并且该TGT 没有过期，就可以使用该TGT 通过票据授权服务器(TGS)完成到任一个服务器的认证而不必重新输入 密码
- B. 认证服务器(AS)和票据授权服务器(TGS)是集中式管理，容易形成瓶颈，系统的性能和安全也 严重依赖于AS和TGS的性能和安全
- C. 该协议通过用户获得票据许可票据、用户获得服务许可票据、用户获得服务三个阶段，仅支持服务器对用户的单向认证
- D. 该协议是一种基于对称密码算法的网络认证协议，随用户数量增加，密钥管理较复杂

回答正确 +1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

98、传输控制协议(TCP)是传输层协议，以下关于TCP 协议的说法，哪个是正确的？（） 分值1分

- A. 相比传输层的另外一个协议UDP，TCP既提供传输可靠性，还同时具有更高的效率，因此具有广泛的用途
- B. TCP协议包头中包含了源IP 地址和目的IP 地址，因此TCP 协议负责将数据传送到正确的主机
- C. TCP协议具有流量控制、数据校验、超时重发、接收确认等机制，因此TCP协议能完全替代IP协议
- D. TCP 协议虽然高可靠，但是相比UDP 协议机制过于复杂，传输效率要比UDP 低

回答正确 +1分

99、以下关于UDP协议的说法，哪个是错误的？（） 分值1分

- A. UDP 具有简单高效的特点，常被攻击者用来实施流量型拒绝服务攻击
- B. UDP协议包头中包含了源端口号和目的端口号，因此UDP 可通过端口号将数据包送达正确的程序
- C. 相比TCP 协议，UDP协议的系统开销更小，因此常用来传送如视频这一类高流量需求的应用数据
- D. UDP 协议不仅具有流量控制，超时重发机制，还能提供加密等服务，因此常用来传输如视频会话这类需要隐私保护的数据

回答正确 +1分

100、由于Internet 的安全问题日益突出，基于TCP/IP 协议，相关组织和专家在协议的不同层次设计了相应的安全通信协议，用来保障网络各层次的安全。其中，属于或依附于传输层的安全协议是（） 分值1分

- A. PP2P
- B. L2TP
- C. SSL
- D. IPSec

回答正确 +1分

收起答题解析

加微信：vic_tom，进cisp考证备考群，请务必备注：备考