CISP练习题一

历史得分

答题人

98

总分100

98

答对

共100题

答题解析 ⌃

全部题目 错题集

姓名：

历史得分

一、单项选择题。（每题1分，共100题，合计100分）

1.某贸易公司的OA系统由于存在系统漏洞，被攻击者上传了木马病毒并删除了系统中的数据，由于系统备份是每周六进行一次，事件发生时间为周三，因此导致该公司三个工作日的数据丢失并使得OA系统在随后两天内无法访问，影响到了与公司有业务往来部分分公司业务，在事故处理报告中，根据GB/Z20986-2007《信息安全事件分级分类指南》，该事件的准确分类和定级应该是（） 分值1分

- A.有害程序事件，特别重大事件（I级）
- B.信息破坏事件，重大事件（II级）
- C.有害程序事件，较大事件（III级）
- D.信息破坏事件，一般事件（IV级）

回答正确 +1分

2.小华在某电子商务公司工作，某天他在查看信息系统设计文档时，发现其中标注该信息系统的RPO《恢复点目标》指标为3小时，请问这意味着（） 分值1分

- A.该信息系统发生重大信息安全事件后，工作人员应在3小时内到位，完成问题定位和应急处理工作
- B.该信息系统发生重大信息安全事件后，工作人员应在3小时内完成应急处理工作，并恢复对外运行
- C.若该信息系统发生重大信息安全事件，工作人员在完成处置和灾难恢复工作后，系统至少能提供3小时的紧急业务服务能力

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● D.若该信息系统发生重大信息安全事件，工作人员在完成处置和灾难恢复工作后，系统至多能丢失3小时的业务数据

回答正确 +1分

3.北京某公司利用SSE-CMM对其自身工程队伍能力进行自我改善，其理解正确的是（） 分值1分

● A.系统安全工程能力成熟度模型（SSE-CMM）定义6个能力级别,当工程队伍不能执行一个过程域中的基本实践时,该过程域的过程能力是0级

○ B.达到SSE-CMM最高级以后，工程队伍执行同一个过程，每次执行的结果质量必须相同

○ C.系统安全工程能力成熟度模型（SSE-MM4）定义了3个风险过程：评价威胁，评价脆弱性，评价影响

○ D.SSE-CMM强调系统安全工程与其他工程学科的区别性和独立性

回答正确 +1分

4.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“本地安全策略”中配置账号策略、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，开启账户策略。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

5.若一个组织声称自己的ISMS符合IS0/IEC27001或GB/T22080标准要求，其信息安全控制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

6.PDCA循环又叫戴明环,是管理学常用的一种模型。关于PDCA四个字母，下面理解

错误的是（） 分值1分

- A.A是Act或Adjust,指持续改进问题
- B.D是Do,指实施、具体运作,实现计划中的内容
- C.C是Check,指检查、总结执行计划的结果,明确效果，找出问题
- D.P是Prepare,指分析问题、发现问题、确定方针、目标和活动计划

回答正确 +1分

7．关于信息安全管理体系的作用,下面理解错误的是（） 分值1分

- A．对内而言,有助于建立起文档化的信息安全管理规范，实现有“法”可依，有章可循，有据可查
- B．对内而言,是一个光花钱不挣钱的事情，需要组织通过其他方面收入来弥补投入
- C．对外而言,有助于使各利益相关方对组织充满信心
- D．对外而言,能起到规范外包工作流程和要求,帮助界定双方各自信息安全责任

回答正确 +1分

8．某集团公司根据业务需要，在各地分支机构部署前置机，为了保证安全，集团总部要求前置机开放，总部服务器采集进行集中分析，在运行过程中发现攻击者也可通过共享从前置机中提取日志，从而导致信息泄露,根据降低攻击面的原则,应采取以下哪项处理措施（） 分值1分

- A.由于共享导致了安全问题,应直接关闭日志共享，禁止总部提取日志进行分析
- B.为配合总部的安全策略,会带来一定的安全问题,但不影响系统使用，因此接受此风险
- C.日志的存在就是安全风险,最好的办法就是取消日志，通过设置让前置机不记录日志
- D.只允许特定的IP地址从前置机提取日志，对日志共享设置访问密码且限定访问的时间

回答正确 +1分

9．不同的信息安全风险评估方法可能得到不同的风险评估结果，所以组织机构应当根据各自的实际情况，选择适当的风险评估方法，下面的描述中错误的是（）。 分值1分

- A.定量风险分析试图从财务数字上对安全风险进行评估，得出可以量化的风险分析结果，以度量风险的可能性和损失量
- B.定量风险分析相比定性风险分析能得到准确的数值，所以在实际工作中应使用定量风险分析，而不应选择定性风险分析
- C.定性风险分析过程中，往往需要凭借分析者的经验直接进行，所以分析结果和风险评估团队的素质、经验和知识技能密切相关
- D.定性风险分析更具主观性，而定量风险分析更具客观性

回答正确 +1分

10.随机进程名称是恶意代码迷惑管理员和系统安全检查人员的技术手段之一，以下对于随机进程名技术，描述正确的是（）。 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ A．随机进程名技术虽然每次进程名都是随机的，但是只要找到了进程名称，就找到了恶意代码程序本身

○ B．恶意代码生成随机进程名称的目的是使进程名称不固定，因为杀毒软件是按照进程名称进行病毒进程查杀

○ C．恶意代码使用随机进程名是通过生成特定格式的进程名称，使进程管理器中看不到恶意代码的进程

● D．随机进程名技术每次启动时随机生成恶意代码进程名称，通过不固定的进程名称使自己不容易被发现真实的恶意代码程序名称

回答正确 +1分

11.软件存在漏洞和缺陷是不可避免的，实践中常使用软件缺陷密度（Defects/KLOC）来衡量软件的安全性.假设某个软件共有29.6万行源代码，总共被检测出145个缺陷，则可以计算出其软件缺陷密度值是（） 分值1分

○ A.0.00049

○ B.0.049

● C.0.49

○ D.49

回答正确 +1分

12.Windows系统中，安全标识符（SID）是标识用户、组和计算机账户的唯一编码，在操作系统内部使用，当授予用户、组、服务或者其他安全主体访问对象的权限时，操作系统会把SID和权限写入对象的ACL中。小刘在学习了SID的组成后，为了巩固所学知识,在自己计算机的Windows操作系统中使用whoami/user操作查看当前用户的SID.得到的SID为S-1-5-21-1534169462-1651380828-111620651-500.下列选项中，关于此SID的理解错误的是（） 分值1分

○ A.前三位S-1-5表示此SID是由WindowsNT颁发的

○ B.第一个子颁发机构是21

○ C.WindowsAT的SID的三个子颁发机构是1534169462、1651380828、111620651

● D.此SID以500结尾,表示内置guest账户

回答正确 +1分

13.保护-检测-响应（Protection-Detection-Response,PDR）模型是（ ）工作中常用的模型，其思想是承认（ ）中漏洞的存在,正视系统面临的（ ）,通过采取适度防护、加强（ ）、落实对安全事件的响应、建立对威胁的防护来保障系统的安全.（） 分值1分

○ A.信息系统；信息安全保障；威胁；检测工作

○ B．信息安全保障；信息系统；检测工作；威胁

● C.信息安全保障；信息系统；威胁；检测工作

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ D．信息安全保障；威胁；信息系统；检测工作

回答正确 +1分

14．老王是某政府信息中心主任。以下哪项项目是符合《保守国家秘密法》要求的（） 分值1分

○ A.老王安排下属小李将损害的涉密计算机的某国外品牌硬盘送到该品牌中国区维修中心修理

○ B.老王要求下属小张把中心所有计算机贴上密级标志

○ C.老王每天晚上12点将涉密计算机连接上互联网更新杀毒软件病毒库

● D.老王提出对加密机和红黑电源智能插座应该与涉密信息系统三同步，合格后方可投入使用

回答正确 +1分

15.信息安全保障技术框架（InformationAssuranceTechnicalFramework,IATF）,目的是为保障政府（）提供了（）信息安全保障技术框架的一个核心思想是（）。深度防御战略的三个核心要素：（）、技术、运行（亦称为操作）。（） 分值1分

● A.信息基础设施；技术指南；深度防御；人员

○ B.技术指南;信息基础设施；深度防御；人员

○ C.信息基础设施;深度防御；技术指南；人员

○ D.信息基础设施;技术指南；人员；深度防御

回答正确 +1分

16.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，该软件用自己的软件名和版本号发给客户端。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httpd.conf中的有关参数

○ C.安装后，删除ApacheHTTPServer源码

○ D．从正确的官方网站下载ApacheHTTPServer，并安装使用

回答正确 +1分

17.有关系统安全工程—能力成熟度模型（SSE-CMM），错误的理解是（） 分值1分

○ A.SSE-CMM要求实施组织与其他组织相互作用，如开发方、产品供应商、集成商和咨询服务商等

○ B.SSE-CMM可以使安全工程成为一个确应的、成熟的和可度量的科目

● C.基于SSE-CMM的工程是独立工程，与软件工程、硬件工程、通信工程等分别规划实施

○ D.SSE-CMM覆盖整个组织的活动，包括管理、组织和工程活动等，而不仅仅是系统安全的工程活动

回答正确 +1分

18.小王在学习定量风险评估方法后，决定试着为单位机房计算火灾的风险大小，假设

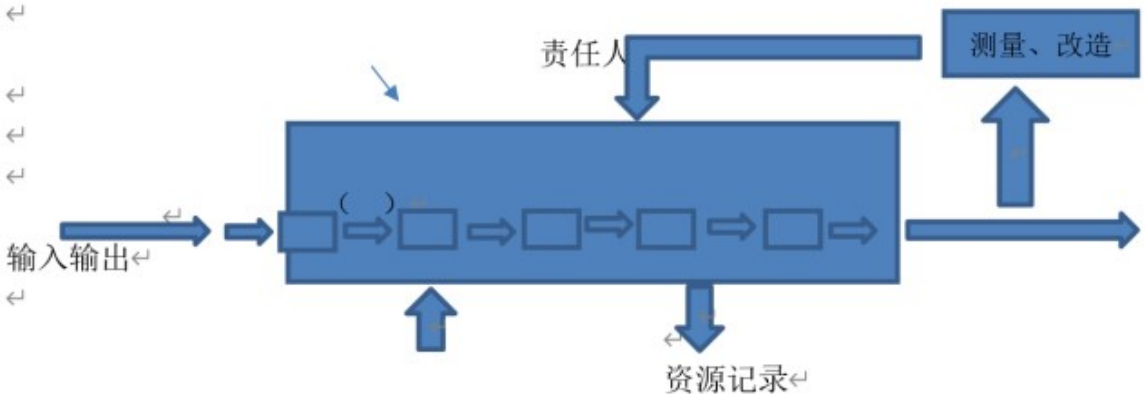
加微信：vic_tom，进cisp考证备考群，请务必备注：备考

单位机房的总价值为400万元人民币，暴露系数（ExposureFactor,EF）是25%,年度发生率（AnnualizedRateofOccurrence,ARO）为0.2,那么小王计算的年度预期损失（AnnualizedLossExpectancy,ALE）应该是（） 分值1分

- A.100万元人民币
- B.400万元人民币
- C.20万元人民币
- D.180万元人民币

回答正确 +1分

19.IS09001-2000标准鼓励在制定、实施质量管理体系以及改进其有效性时采用过程方法，通过满足顾客要求，增进顾客满意度，下图是关于过程方法的示意图，图中括号空白处应填写（ ）



分值1分

- A.策略
- B.管理者
- C.组织
- D.活动

回答错误 +0分

正确答案:

D.活动

20.信息安全组织的管理涉及内部组织和外部各方两个控制目标。为了实现对组织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

回答错误 +0分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

正确答案:

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

21.在信息安全风险管理过程中，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

22．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

回答正确 +1分

23.应急响应是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，也包括事件发生后的应对措施

○ B.应急响应工作有其鲜明的特点：具有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.应急响应是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置和整体协调的重要性

回答正确 +1分

24.若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T22080标准要求，其信息安

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

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、物理和环境安全、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

25.在国家标准GB/T20274.1-2006《信息安全技术信息系统安全保障评估框架第一部分：简介和一般模型》中，信息系统安全保障模型包含哪几个方面（） 分值1分

- A.保障要素、生命周期和运行维护
- B.保障要素、生命周期和安全特征
- C.规划组织、生命周期和安全特征
- D.规划组织、生命周期和运行维护

回答正确 +1分

26.有关危害国家秘密安全的行为包括（） 分值1分

- A.严重违反保密规定行为，定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为、保密行政管理部门的工作人员的违法行为
- B.严重违反保密规定行为、公共信息网络运营商及服务商不履行保密义务的行为，保密行政管理部门的工作人员的违法行为，但不包括定密不当行为
- C.严重违反保密规定行为、定密不当行为、保密行政管理部门的工作人员的违法行为，但不包括公共信息网络运营商及服务商不履行保密义务的行为
- D.严重违反保密规定行为，定密不当行为、公共信息网络运营商及服务商不履行保密义务的行为、但不包括保密行政管理部门的工作人员的违法行为

回答正确 +1分

27.私有IP地址是一段保留的IP地址。只使用在局域网中，无法在Internet上使用。关于私有地址，下面描述正确的是（） 分值1分

- A.A类和B类地址中没有私有地址，C类地址中可以设置私有地址
- B.A类地址中没有私有地址，B类和C类地址中可以设置私有地址
- C.A类、B类和C类地址中都可以设置私有地址
- D.A类、B类和C类地址中都没有私有地址

回答正确 +1分

28.《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号明确了我国信息安全保障工作的（）、加强信息安全保障工作的（）、需要重点加强的信息安全保障工作。27号文的重大意义是，它标志着我国信息安信息安全保障工作

有了（）、我国最近十余年的信息安全保障工作都是围绕此政策性文件来（）的、促进了我国（）的各项工作。（） 分值1分

- A.方针；主要原则；总体纲领；展开和推进；信息安全保障建设
- B.总体要求；总体纲领；主要原则；展开；信息安全保障建设
- C.方针和总体要求;主要原则；总体纲领；展开和推进；信息安全保障建设
- D.总体要求；主要原则；总体纲领；展开；信息安全保障建设

回答正确 +1分

29.信息系统建设完成后，到达（）的信息系统的运营使用单位应当选择符合国家规定的测评机构，进行测评合格后方可投入使用。（） 分值1分

- A.二级以上
- B.三级以上
- C.四级以上
- D.五级以上

回答正确 +1分

30.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

31.有关系统工程的特点说法错误的是（） 分值1分

- A.系统工程是基本理论的技术实现
- B.系统工程是一种对所有系统都具有普遍意义的科学方法
- C.系统工程是织管理系统规划、研究、制造、试验、使用的科学方法
- D.系统工程是一种方法论

回答正确 +1分

32．按照我国信息安全等级保护的有关政策和标准，有些信息系统只需要自主定级、自主保护,按照要求向公安机关备案即可,可以不需要上级或主管部门来测评和检查.此类信息系统属于（）。 分值1分

- A．零级系统
- B．一级系统

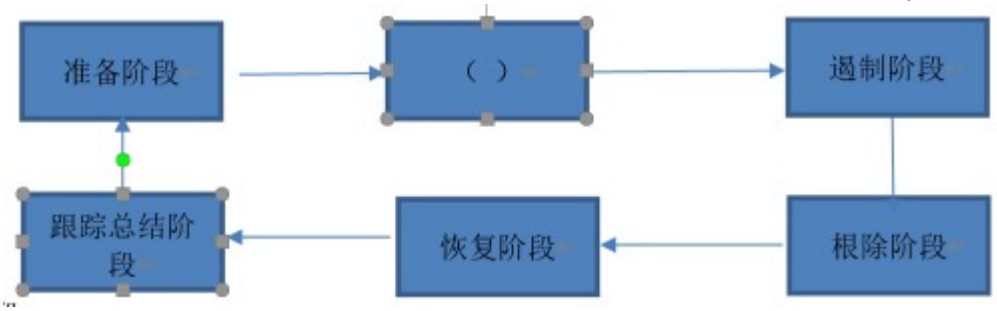
加微信：vic_tom，进cisp考证备考群，请务必备注：备考

C．二级系统

D．三级系统

回答正确 +1分

33.为了能够合理、有序地处理安全事件，应该先制定出事件应急响应方法和过程，有助于一个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低.PDCERF方法论是一种广泛使用的方法，其将应急响应分成六个阶段，如下图所示，请为图中括号空白处选择合适的内容（ ）



分值1分

A.培训阶段

B.文档阶段

C.报告阶段

D.检测阶段

回答正确 +1分

34.信息安全管理体系（ISMS)的建设和实施是一个组织的战略性举措，若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T22080标准要求，则需实施准确要求，并需要实施以下ISMS建设的各项工作，哪一项不属于ISMS建设的工作（） 分值1分

A.规划与建立ISMS

B.实施和运行ISMS

C.监视和评审ISMS

D.保持和审核ISMS

回答正确 +1分

35.在某次信息安全应急响应过程中，小王正在实施如下措施：消除或阻断攻击源、找到并消除系统的脆弱性/漏洞、修改安全策略、加强防范措施、格式化被感染恶意程序的介质等。请问，按照PDCERF应急响应方法，这些工作应处于以下哪个阶段（）
分值1分

A.准备阶段

B.检测阶段

C.遏制阶段

D.根除阶段

回答正确 +1分

36.关于<网络安全法>域外适用效力的理解，以下哪项是错误的 分值1分

- A.当前对于境外的网络攻击，我国只能通过向来源国采取抗议
- B.对于来自境外的网络安全威胁我国可以组织技术力量进行监测、防御和处置
- C.对于来自境外的违法信息我国可以加以阻断传播
- D.对于来自境外的网络攻击我国可以追究其法律责任

回答正确 +1分

37.规范的实施流程和文档管理，是信息安全风险评估能否取得成功的重要基础。某单位在实施风险评估时，形成了《待评估信息系统相关设备及资产清单》。在风险评估实施的各个阶段中，该《待评估信息系统相关设备及资产清单》应是如下（）中的输出结果。（） 分值1分

- A.风险评估准备
- B风险要素识别
- C风险分析
- D:风险结果判定

回答正确 +1分

38有关危害国家秘密安全的行为的法律责任,正确的是（） 分值1分

- A严重违反保密规定行为只要发生,无论是否产生泄密实际后果,都要依法追究责任
- B.非法获取国家秘密.不会构成刑事犯罪.不需要承担刑事责任
- C.过失泄露国家秘密，不会构成刑事犯罪.不需要承担刑事责任
- D.承担了刑事责任,无需在承担行政责任和/或其他处分

回答正确 +1分

39.作为信息安全从业人员,以下哪种行为违反了CISP职业道德准则（） 分值1分

- A抵制通过网络系统侵犯公公合法权益
- B通过公众网络传播非法软件
- C不在计算机网络系统中进行造谣、欺诈、诽谤等活动
- D帮助和指导信息安全同行提升信息安全保障知识和能力

回答正确 +1分

40.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除了用户名口令认证方式外,还加入基于数字证书的身份认证功能,同时用户口令使用SHA-1算法加密后存放在后台数据库中,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.最小特权原则
- B.职责分离原则

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● C纵深防御原则

○ D.最少共享机制原则

回答正确 +1分

41.防火墙是网络信息系统建设中经常采用的一类产品，它在内外网隔离方面的作用是（） 分值1分

○ A.既能物理隔离，又能逻辑隔离

○ B能物理隔离，但不能逻辑隔离

● C.不能物理隔离，但是能逻辑隔离

○ D.不能物理隔离，也不能逻辑隔离

回答正确 +1分

42.关于计算机取证描述不正确的是（） 分值1分

○ A计算机取证是使用先进的技术和工具，按照标准规程全面地检查计算机系统，以提取和保护有关计算机犯罪的相关证据的活动

○ B取证的目的包括:通过证据查找肇事者.通过证据推断犯罪过程,通过证据判断受害者损失程度及收集证据提供法律支持.

● C电子证据是计算机系统运行过程中产生的各种信息记录及存储的电子化资料及物品.对于电子证据,取证工作主要围绕两方面进行:证据的获取和证据的保护

○ D计算机取证的过程可以分为准备、保护、提取、分析和提交5个步骤

回答正确 +1分

43.为推动和规范我国信息安全等级保护工作，我国制定和发布了信息安全等级保护工作所需要的一系列标准,这些标准可以按照等级保护工作的工作阶段大致分类.下面四个标准中，（）提出和规定了不同安全保护等级信息系统的最低保护要求,并按照技术和管理两个方面提出了相关基本安全要求。（） 分值1分

● A.GB/T22239-2019《网络安全等级保护基本要求》

○ B.GB/T22240-2008《信息系统安全保护等级定级指南》

○ C.GB/T25070-2010《信息系统等级保护安全设计技术要求》

○ D.GB/T28449-2012《信息系统安全等级保护测评过程指南》

回答正确 +1分

44.自主访问控制模型（DAC）的访向控制关系可以用访问控制表(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（ ）。 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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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

45.你是单位安全主管，由于微软刚发布了数个系统漏洞补丁，安全运维人员给出了针对此批漏洞修补的四个建议方案，请选择其中一个最优方案执行（） 分值1分

○ A.由于本次发布的数个漏洞都属于高危漏洞，为了避免安全风险，应对单位所有的服务器和客产端尽快安装补丁

○ B.本次发布的漏洞目前尚未出现利用工具，因此不会对系统产生实质性危害，所以可以先不做处理

● C.对于重要的服务，应在测试环境中安装并确认补丁兼容性问题后再在正式生产环境中部署

○ D.对于服务器等重要设备，立即使用系统更新功能安装这批补丁，用户终端计算机由于没有重要数据，由终端自行

回答正确 +1分

46.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制模型的设计思路。如果想要为一个存在大量用户的信息系统实现自主访向控制功能，在以下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

47.以下关于项目的含义,理解错误的是（） 分值1分

○ A项目是为达到特定的目的，使用一定资源、在确定的期间内、为特定发起人而提供独特的产品、服务或成果而进行的一次性努力

● B.项目有明确的开始日期，结束日期由项目的领导者根据项目进度来随机确定

○ C项目资源指完成项目所需要的人,财,物等

○ D:项目目标要遵守SMART原则，即项目的目标要求具体(Specific)、可测量(Measurable)、需相关方的一致同意(Agreeto)、现实(Realistic)、有定的时限(Time-oriented)

回答正确 +1分

48关于标准,下面哪项理解是错误的（） 分值1分

○ A标准是在一定范围内为了获得最佳秩序，经协商一致制定并由公认机构批准，共同重复使用的一种规范性文件。

● B.国际标准是由国际标准化组织通过并公开发布的标准。同样是强制性标准，当国家标准和国际标

准的条款发生冲突时,应以国际标准条约为准.

○ C行业标准是针对没有国家标准而又需要在全国某个行业范围内统一的技术要求而制定的标准.同样是强制性标准,当行业标准和国家标准的条款发生冲突时,应以国家标准条款为准

○ D.地方标准由省、自治区、直辖市标准化行政主管部门制定，并报国务院标准化行政主管部门和国务院有关行政主管部门备案，在公布国家标准之后，该地方标准即应废止

回答正确 +1分

49.分布式拒绝服务(DistributedDenialofService,DDoS)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。一般来说，DDOS攻击的主要目的是破坏目标系统的（） 分值1分

○ A.保密性

○ B.完整性

● C.可用性

○ D.真实性

回答正确 +1分

50.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，根据任务安排，他使用了Nessus工具来扫描和发现数据库服务器的漏洞。根据风险管理的相关理论，他这个扫描活动属于下面哪一个阶段的工作（） 分值1分

○ A.风险分析

● B.风险要素识别

○ C.风险结果判定

○ D.风险处理

回答正确 +1分

51.GB/T22080200《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，即信息安全管理体系应包括建立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

52.关于信息安全应急响应管理过程描述不正确的是（） 分值1分

○ A.基于应急响应工作的特点和事件的不规则性，事先制定出事件应急响应方法和过程，有助于一个

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降至最低

○ B.应急响应方法和过程并不是唯一的

○ C.一种被广为接受的应急响应方法是将应急响应管理过程分为准备、检测、遏制、根除、恢复和跟踪总结6个阶

● D.一种被广为接受的应急响应方法是将应急响应管理过程分为准备、检测、遏制、根除、恢复和跟踪总结6个阶段的响应方法一定能确保事件处理的成功

回答正确 +1分

53.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/18336.1－２００６）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．可跟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

54.有关能力成熟度模型（CMM）,理解错误的是（Ａ） 分值1分

● Ａ．CMM的基本思想是，因为问题是由技术落后引起的，所以新技术的运用会在一定程度上提高质量，生产率和利润率

○ Ｂ．CMM的思想源于项目管理和质量管理

○ Ｃ.CMM是一种衡量工程实施能力的方法，是一种面相工程过程的方法．

○ Ｄ.CMM是建立在统计过程控制理论基础上的，它基于这样一个假设，即“生产过程的高质量和在过程中组织实施的成熟性可以低成本地生产出高质量产品”

回答正确 +1分

55.某信息安全公司的团队对某款名为“红包快抢”的外挂进行分析，发现此外挂是一个典型的木马后门，使黑客能够获得受害者电脑的访问权．该后门程序为了达到长期驻留在受害者的计算机中，通过修改注册表启动项来达到后门程序随受害者计算机系统启动而启动，为防范此类木马后门的攻击，以下做法无用的是（）
Ａ不下载，不执行，不接收来历不明的软件或文件 分值1分

○ B.不随意打开来历不明的邮件，不浏览不健康不正规的网站

● C.使用用户名和密码信息

○ D.安装反病毒软件和防火墙，安装专门的木马防治软件

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

56.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，根据任务安排，他依据已有的资产列表，逐个分析可能危害这些资产的主体，动机，途径等多种因素，分析这些因素出现及造成损失的可能性大小，并为其赋值。请问，他这个工作属于下面哪一个阶段的工作（） 分值1分

- A.资产识别并赋值
- B.脆弱性识别并赋值
- C.威胁识别并赋值
- D.确认已有的安全措施并赋值

回答正确 +1分

57.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

58.有关系统安全工程-能力成熟度模型(SSE-CMM)中的通用实施(GenericPractices,GP)，错误的理解是（） 分值1分

- A.GP是涉及过程的管理、测量和制度化方面的活动
- B.GP适用于域维中部分过程区域(ProcessAreas,PA)的活动而非所有PA的活动
- C.在工程实施时，GP应该作为基本实施(BasePractices,BP)的一部分加以执行
- D.在评估时，GP用于判定工程组织执行某个PA的能力

回答正确 +1分

59.为保障信息系统的安全，某经营公众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描述报告。关于此项工作,下面说法错误的是（）。 分值1分

- A.信息安全需求报告应依据该公众服务信息系统的功能设计方案为主要内容来撰写
- B.信息安全需求描述报告是设计和撰写信息安全保障方案的前提和依据
- C.信息安全需求描述报告应当基于信息安全风险评估结果和有关政策法规和标准的合规性要求得到
- D.信息安全需求描述报告的主体内容可以按照技术、管理和工程等方面需求展开编写

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

60.若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T22080标准要求，其信息安全控制措施通常需要在符合性方面实施常规控制。符合性常规控制这一领域不包括以下哪项控制目标（） 分值1分

- A.符合法律要求
- B.符合安全策略和标准以及技术符合性
- C.信息系统审核考虑
- D.访问控制的业务要求、用户访问管理

回答正确 +1分

61.恢复时间目标(RecoveryTimeobjective,RTO)和恢复点目标(RecoveryPointObieetive,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

62.某网络安全公司基于网络的实时入侵检测技术,动态监测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为,会及时响应,并通知防火墙实时阻断攻击源从而进步提高了系统的抗攻击能力更有效地保护了网络资源,提高了防御体系级别。但入侵检测技术不能实现以下哪种功能（） 分值1分

- A.检测并分析用户和系统的活动
- B.核查系统的配置漏洞，评估系统关键资源和数据文件的完整性
- C.防止IP地址欺骗
- D.识别违反安全策略的用户活动

回答正确 +1分

63.对信息安全事件的分级参考下列三个要素:信息系统的重要程度、系统损失和社会影响。依据信息系统的重要程度对信息系统进行划分，不属于正确划分级别的是（） 分值1分

- A特别重要信息系统
- B.重要信息系统
- C.一般信息系统
- D.关键信息系统

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

64.以下关于威胁建模流程步骤说法不正确的是（） 分值1分

- A.威胁建模主要流程包括四步:确定建模对象、识别威胁、评估威胁和消减威胁
- B.评估威胁是对威胁进行分析，评估被利用和攻击发生的概率，了解被攻击后资产的受损后果，并计算风险
- C.消减威胁是根据威胁的评估结果，确定是否要消除该威胁以及消减的技术措施，可以通过重新设计直接消除威胁，或设计采用技术手段来消减威胁
- D.识别威胁是发现组件或进程存在的威胁，它可能是恶意的，也可能不是恶意的，威胁就是漏洞

回答正确 +1分

65.CC标准是目前系统安全认证方面最权威的标准，以下哪项没有体现CC标准的先进性（） 分值1分

- A.结构的开放性，即功能和保证要求都可以在具体的“保护轮廓"和“安全目标”中进一步细化和扩展
- B.表达方式的通用性，即给出通用的表达方式
- C.独立性，它强调将安全的功能和保证分离
- D.实用性，将CC的安全性要求具体应用到IT产品的开发、生产、测试和评估过程中

回答正确 +1分

66.一个信息管理系统通常会对用户进行分组并实施访问控制。例如，在一个学校的教务系统中，教师能够录入学生的考试成绩，学生只能查看自己的分数，而学校教务部门的管理人员能够对课程信息、学生的选课信息等内容进行修改。下列选项中，对访问控制的作用的理解错误的是（）。 分值1分

- A.对经过身份鉴别后的合法用户提供所有服务
- B.拒绝非法用户的非授权访问请求
- C.在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理
- D.防止对信息的非授权篡改和滥用

回答正确 +1分

67.GaryMcGraw博士及其合作者提出软件安全应由三根支柱来支撑，这三个支柱是（） 分值1分

- A.源代码审核、风险分析和渗透测试
- B.应用风险管理、软件安全接触点和安全知识
- C.威胁建模、渗透测试和软件安全接触点
- D.威胁建模、源代码审核和模糊测试

回答正确 +1分

68.部署互联网协议安全虚拟专用网(InternetProtocolSecurityVirtualPrivateNetwork,IP

secVPN)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IPsecVPN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(SecurityAuthentication,SA)资源的消耗
- D.报文验证头协议(AuthenticationHeader,AH)可以提供数据机密性

回答正确 +1分

69.Linux系统的安全设置主要从磁盘分区、账户安全设置、禁用危险服务、远程登录安全、用户鉴别安全、审计策略、保护root账户、使用网络防火墙和文件权限操作共10个方面来完成。小张在学习了Linux系统安全的相关知识后，尝试为自己计算机上的L.inux系统进行安全配理。下列选项是他的部分操作,其中不合理的是（） 分值1分

- A编辑文件/etc/passwd,检查文件中用户ID,禁用所有ID=0的用户
- B.编辑文件/etc/ssh/sshd.config,将PermitRoot设置为no
- C.编辑文件/etc/pam.d/system-auth,设置authrequiredpam_tally,soonerrfalldeny 6 unlock_time=300
- D.编辑文件/etc/profile,设置TMOUT=600

回答正确 +1分

70.以下关于互联网协议安全(internetprotocolSourity,IPsec)协议说法错误的是（）
分值1分

- A.在传送模式中，保护的是IP负载
- B验证协议(Authentication Head,AII)和IP封装安全载荷协议(Encapsulatin Security Payload,ESP都能以传输模式和隧道模式工作
- C在隧道模式中，保护的是整个互联网协议(InternetProtocol,,IP)包,包括IP头
- D.IPsec仅能保证传输数据的可认证性和保密性

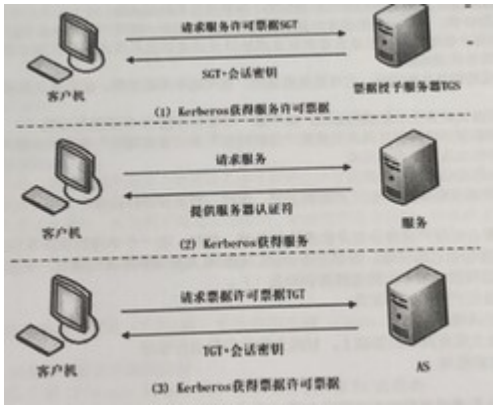
回答正确 +1分

71.在信息系统中，访问控制是重要的安全功能之一.它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。访间控制模型将实体划分为主体和客体两类，通过对主体身合的识别来限制其对客体的访问权展。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.主体可以接收客体的信息和数据，也可以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.对目录的访问权限可分为读、写和拒绝访问

回答正确 +1分

72.Kerberos协议是常用的集中访问控制协议，通过可信第三方的认证服务，减轻应用服务器的负担。Kerberos的运行环境由密钥分发中心（）:应用服务器和客户端三个部分组成。其中，KDC分为认证服务器AS和票据授权服务器TGS两部分.下图展示了kerberos协议的三个阶段,分别是(1)kerberos获得服务许可票据,(2)kerberos获得服务,(3)kerberos获得票据许可票据.下列选项中,对这三个阶段的排序正确的是（）



分值1分

- A(1)→(2)→(3)
- B.(3)→(2)→(1)
- C.(2)—(1)→(3)
- D.(3)→(1)→(2)

回答正确 +1分

73.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V1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计算几个风险值（）

分值1分

- A.2
- B.3
- C.5
- D.6

回答正确 +1分

74.规范形成了若干文档，其中,下面（）中的文档应属于风险评估中"风险要素识别"阶段输出的文档.（） 分值1分

- A.《风险评估方案》，主要包括本次风险评估的目的、范围、目标、评估步骤、经费预算和进度安排等内容
- B.《风险评估方法和工具列表》,主要包括拟用的风险评估方法和测试评估工具等内容
- C.《风险评估准则要求》,主要包括现有风险评估参考标准,采用的风险分析方法,资产分类标准等内容

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● D.《已有安全措施列表》，主要包括经检查确认后的已有技术和管理各方面安全措施等内容

回答正确 +1分

75.小李在某单位是负责信息安全风险管理方面的工作的部门领导,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,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分析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

76.关于WiFi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是有线局城安全协议，而WPA2是无线局城网协议

○ B.WPA是适用于中国的无线局域安全协议，而WPA2是适用于全世界的无线局城网协议

○ 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

77.从Linux内核2.1版开始，实现了基于权能的特权管理机制,实现了对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设计特权操作时，仍然通过setuid实现

回答正确 +1分

78.小李在检查公司对外服务网站的源代码时，发现程序在发生诸如没有找到资源、数据库连接错误、写临时文件错误等问题时，会将详细的错误原因在结果页面上显示出来。从安全角度考虑，小李决定修改代码，将详细的错误原因都隐藏起来，在页面上仅仅告知用户“抱歉，发生内部错误”.请问，这种处理方法的主要目的是（） 分值1分

○ A.避免缓冲区溢出

○ B.安全处理系统异常

○ C.安全使用临时文件

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

● D.最小化反馈信息

回答正确 +1分

79.以下关于灾难恢复和数据备份的理解，说法正确的是（） 分值1分

○ A.增量备份是备份从上次完全备份后更新的全部数据文件

○ B.依据具备的灾难恢复资源程度的不同，灾难恢复能力分为7个等级

● C.数据备份按数据类型划分可以划分为操作系统数据备份和用户数据备份

○ D.如果系统在一段时间内没有出现问题，就可以不用再进行容灾演练了

回答正确 +1分

80.关于信息安全事件管理和应急响应，以下说法错误的是（） 分值1分

○ A.应急响应是指组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施

● B.应急响应方法，将应急响应管理过程分为遏制、根除、处置、恢复、报告和跟踪6个阶段

○ C.对信息安全事件的分级主要参考信息系统的重要程度、系统损失和社会影响三方面因素

○ D.根据信息安全事件的分级参考要素，可将信息安全事件划分为4个级别:特别重大事件(I级)、重大事件(II级)、较大事件(II级)和一般事件(IV级)

回答正确 +1分

81.若一个组织声称自己的ISMS符合ISO/IEC27001或GB/T22080标准要求，其信息安全控制措施通常需要在物理和环境安全方面实施常规控制。物理和环境安全领域包括安全区域和设备安全两个控制目标。安全区域的控制目标是防止对组织场所和信息的未授权物理访问、损坏和干扰，关键或敏感的信息及信息处理设施应放在安全区域内，并受到相应保护，该目标可以通过以下控制措施来实现，不包括哪-项（）
分值1分

○ A.物理安全边界、物理入口控制

○ B.办公室、房间和设施的安全保护，外部和环境威胁的安全防护

○ C.在安全区域工作，公共访问、交接区安全

● D.人力资源安全、物理环境安全、通信安全等

回答正确 +1分

82.根据《关于开展信息安全风险评估工作的意见》的规定，错误的是（）。
分值1分

● A.信息安全风险评估分自评估、检查评估两形式。应以检查评估为主，自评估和检查评估相互结合、互为补充

○ B.信息安全风险评估工作要按照“严密组织、规范操作、讲求科学、注重实效”的原则开展

○ C信息安全风险评估应贯穿于网络和信息系统建设运行的全过程

○ D.开展信息安全风险评估工作应加强信息安全风险评估工作的组织领导

回答正确 +1分

83.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威胁,包括恶意攻击和恶作剧攻击者,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

84.数据在进行传输前，需要由协议栈自上面下对数据进行封装。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

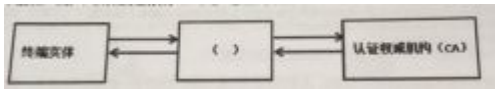
● B.传输层、互联网络层、网络接口层

○ 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

85.公钥基础设施(Public Key Infrastructure,PKI)引入数字证书的概念，用来表示用户的身份。下图简要地描述了终端实体(用户)从认证权威机构CA申请、撤销和更新数字证书的流程。请为中间框空白处选择合的选项（）



分值1分

○ A.证书库

● B.RA

○ C.0CSP

○ D.CRL库

回答正确 +1分

86.关于信息安全管理体系(InformationSecurityManagementSystems,ISMS)，下面描

述错误的是（） 分值1分

○ A.信息安全管理体系是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系，包括组织架构、方针、活动、职责及相关实践要素

○ B.管理体系(ManagesentSystems)是为达到组织目标的策略、程序、指南和相关资源的框架，信息安全管理体系是管理体系思想和方法在信息安全领域的应用

○ C.概念上，信息安全管理体系有广义和狭义之分，狭义的信息安全管理体系是指按照IS027001标准定义的管理体系，它是一个组织整体管理体系的组成部分

● D.同其他管理体系一样，信息安全管理体系也要建立信息安全管理组织机构、健全信息安全管理制度、构建信息安全技术防护体系和加强人员的安全意识等内容

回答正确 +1分

87.由于密码技术都依赖于密钥，因此密钥的安全管理是密码技术应用中非常重要的环节，下列关于密钥管理说法错误的是（） 分值1分

○ A.科克霍夫在《军事密码学》中指出系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥

● B.在保密通信过程中，通信双方可以一直使用之前用过的会话密钥，不影响安全性

○ C.密钥管理需要在安全策略的指导下处理密钥生命周期的整个过程，包括产生、存储、备份、分配、更新、撤销等

○ D.在保密通信过程中，通信双方也可利用Diffie-Hellman协议协商出会话密钥进行保密通信

回答正确 +1分

88.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-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

89.金女士经常通过计算机在互联网上购物，从安全角度看，下面哪项是不好的操作习惯（） 分值1分

● A.使用专用上网购物用计算机，安装好软件后不要对该计算机上的系统软件、应用软件进行升级

○ B.为计算机安装具有良好声誉的安全防护软件,包括病毒查杀,安全检查和安全加固方面的软件.

○ C.在IE的配置中,设置只能下载和安装经过签名的,安全的ActiveX控件

○ D.在使用网络浏览器时,设置不在计算机中保留网络历时记录和表单数据

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

90.某集团公司信息安全管理员根据领导安排制定了下一年度的培训工作计划,提出了四大培训任务和目标,关于这四个培训任务和目标,作为主管领导,以下选项中合理的是（） 分值1分

○ A.由于网络安全上升到国家安全的高度,网络安全必须得到足够的重视,因此安排了对集团公司下属单位的总经理(一把手)的网络安全法培训

○ B.对下级单位的网络安全管理岗人员实施全面安排培训,建议通过CISP培训以确保人员能力得到保障

○ C.对其他信息化相关人员(网络管理员,软件开发人员)也进行安全基础培训,使相关人员对网络安全有所了解

● D.对全体员工安排信息安全意识及基础安全知识培训,实现全员信息安全意识教育

回答正确 +1分

91.某国贸公司信息安全管理员考虑到信息系统对业务影响越来越重要,计划编制本单位信息安全应急响预案,在向主管领导写报告时,他列举了编制信息安全应急预案的好处和重要性,在他罗列的四条理由中,其中不适合作为理由的一条是（） 分值1分

○ A.应急预案是明确关键业务系统信息安全应急响应指挥体系和工作机制的重要方式

○ B.应急预案是提高应对网络和信息系统突发事件能力,减少突发事件造成的损失和危害,保障信息系统运行平稳,安全,有序,高效的手段

● C.编制应急预案是国家网络安全法对所有单位的强制要求,因此必须建设

○ D.应急预案是保障单位业务系统信息安全的重要举措

回答正确 +1分

92.小王在学习信息安全管理体系相关知识后,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,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涉及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

93.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IS027001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，应由信息技术责任部门(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

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

○ 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，也应传达到客户、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，并确认接受相关残余风险

回答正确 +1分

94.《信息安全保障技术框架》(InformationAssuranceTechnicalFramework,IATF)是由（）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

95.应急响应是信息安全事件管理的重要内容。基于应急响应工作的特点和事件的不规则性，事先制定出事件应急响应方法和过程，有助于个组织在事件发生时阻止混乱的发生或是在混乱状态中迅速恢复控制，将损失和负面影响降到最低。应急响应方法和过程并不是唯一-的。-种被广为接受的应急响应方法是将应急响应管理过程分为6个阶段，为准备->检测->遏制->根除->恢复->跟踪总结。请问下列说法有关于信息安全应急响应管理过程错误的是（ C ）。 分值1分

○ A.确定重要资产和风险，实施针对风险的防护措施是信息安全应急响应规划过程中最关键的步骤

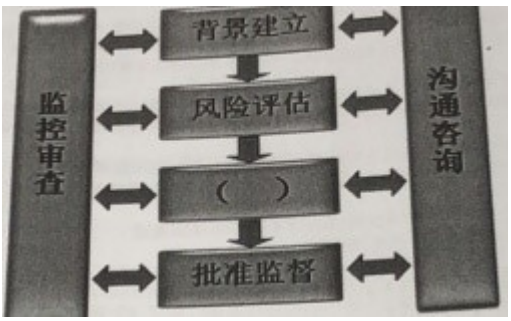
○ B.在检测阶段,首先要进行监测,报告及信息收集

● C.遏制措施可能会因为时间的类别和级别不同而完全不同,常见的遏制措施有:完全关闭所有系统,拔掉网线等

○ D.应按照应急响应计划中事先制定的业务恢复优先顺序和回复步骤,顺次恢复相关的系统

回答正确 +1分

96.我国标准《信息安全风险管理指南》(GB/Z2361)给出了信息安全风险管理的内容和过程,可以用下图来表示,图中空白处应该填写（ ）



分值1分

○ A.风险计算

○ B.风险评价

○ C.风险预测

● D.风险处理

回答正确 +1分

97.即使最好用的安全产品也存在（）的结果，在任何的系统中敌手最终都能够找出一个被开发出的漏洞。一种有效的对策是在敌手和它的目标之间配备多种（）。每一种机制都应包括（）两种手段。（） 分值1分

○ A.安全机制:安全缺陷:保护和检测

● B.安全缺陷:安全机制;保护和检测

○ C.安全缺陷;保护和检测;安全机制

○ D.安全缺陷;安全机制;外边和内部

回答正确 +1分

98.某IT公司针对信息安全事件已经建立了完善的预案，在年度企业信息安全总结会上，信息安全管理员对今年应急预案工作做出了四个总结，其中有一项总结工作是错误，作为企业的CSO,请你指出存在问题的是哪个总结？() 分值1分

● A.公司自身拥有优秀的技术人员，系统也是自己开发的，无需进行应急演练工作，因此今年的仅制定了应急演练相关流程及文档，为了不影响业务，应急演练工作不举行

○ B.公司制定的应急演练流程包括应急事件通报、确定应急事件优先级、应急响应启动实施、应急响应时间后期运维、更新现有应急预案五个阶段，流程完善可用

○ C.公司应急预案包括了基础环境类、业务系统类、安全事件类和其他类，基本覆盖了各类应急事件类型

○ D.公司应急预案对事件分类依据GB/Z20986-2007《信息安全技术信息安全事件分类分级指南》，分为7个基本类别，预案符合国家相关标准

回答正确 +1分

99.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

100. 以下哪一项不是我国信息安全保障工作的主要目标： （） 分值1分

加微信：vic_tom，进cisp考证备考群，请务必备注：备考

- ○ A、保障和促进信息化发展
- ○ B、维护企业与公民的合法权益
- ● C、构建高效的信息传播渠道
- ○ D、保护互联网知识产权

回答正确 +1分

收起答题解析