

**CISP练习题二**

校花费

答题人

100

100

答对

总分100

共100题

**答题解析 ✎****全部题目** **错题集**

姓名：

校花费

一、单项选择题。（每题1分，共100题，合计100分）

1.分布式拒绝服务（DistributedDenialofServiceDDoS）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，对一个或多个目标成功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

2.根据《信息安全等级保护管理办法》、《关于开展信息安全等级保护测评体系建设试点工作的通知》（公信安【2009】812号），关于推动信息安全等级保护（）建设和开展（）工作的通知（公信安【2010】303号）等文件，由公安部（）对等级保护测评机构管理，接受测评机构的申请、考核和定期（），对不具备能力的测评机构则

() 分值1分

- A.等级测评；测评体系；等级保护评估中心；能力验证；取消授权
- B.测评体系；等级保护评估中心；等级测评；能力验证；取消授权
- C.测评体系；等级测评；等级保护评估中心；能力验证；取消授权

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- D.测评体系；等级保护评估中心；能力验证；等级评估；取消授权

 回答正确

+1分

3.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果的重要基础，某单位在实施风险评估时，按照规范成了若干文档，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，要素分类标准等内容。
- D.《已有安全措施列表》，主要包括经验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

4.某购物网站开发项目过需要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，请问以上安全设计的是哪项安全设计原则（） 分值1分

- A.小原最小特权原则
- B.职责分离原则
- C.纵深防御原则
- D.最少共享机制原则

 回答正确

+1分

5.以下哪个是国际信息安全标准化组织的简称（） 分值1分

- A.ANST
- B.ISO
- C.IEEE
- D.NIST

 回答正确

+1分

6.某银行网上交易系统开发项目在设计阶段分析系统运行过程中可能存在的攻击，请问以下拟采取的安全措施中，哪一项不能降低该系统的受攻击面（） 分值1分

- A.远程用户访问需进行身份认证
- B.远程用户访问时具有管理员权限
- C.关闭服务器端不必要的系统服务
- D.当用户访问其账户信息时使用严格的身份认证机制

 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**

7.信息系统建设完成后，（）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

8.某单位根据业务需要准备立项开发一个业务软件，对于软件开发安全投入经费研讨时开发部门和信息中心就发生了分歧，开发部门认为开发阶段无需投入，软件开发完成后发现问题后再针对性的解决，比前期安全投入要成本更低；信息中心则认为应在软件安全开发阶段投入，后期解决代价太大，双方争执不下，作为信息安全专家，请选择对软件开发安全投入的准确说法（） 分值1分

- A.信息中心的考虑是正确的，在软件立项投入解决软件安全问题，总体经费投入比软件运行后的费用要低
- B.软件开发部门的说法是正确的，因为软件发现问题后更清楚问题所在，安排人员进行代码修订更简单，因此费用更低
- C.双方的说法都正确，需要根据具体情况分析是开发阶段投入解决问题还是在上线后再解决问题费用更低
- D.双方的说法都错误，软件安全问题在任何时候投入解决都可以，只要是一样的问题，解决的代价相同

 回答正确

+1分

9.下列我国哪一个政策性文件明确了我国信息安全保障工作的方针和总体要求以及加强信息安全保障工作的主要原则（） 分值1分

- A.《关于加强政府信息系统安全和保密管理工作的通知》
- B.《中华人民共和国计算机信息系统安全保护条例》
- C.《国家信息化领导小组关于加强信息安全保障工作的意见》
- D.《关于开展信息安全风险评估工作的意见》

 回答正确

+1分

10.由于频繁出现软件运行时被黑客远程攻击获取数据的现象，某软件公司准备加强软件安全开发管理，在下面做法中，对于解决问题没有直接帮助的是（） 分值1分

- A.要求开发人员采用瀑布开发模型进行开发
- B.要求所有的开发人员参加软件安全意识培训
- C.要求规范软件编码，并制定公司的安全编码准则
- D.要求增加软件安全测试环节，尽早发现软件安全问题

 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

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

11.访问控制是对用户或用户组访问本地或网络上的域资源进行授权的一种机制。在Windows2000以后的操作系统版本中，访问控制是一种双重机制，它对用户的授权基于用户权限和对象许可，通常使用ACL、访问令牌和授权管理器来实现访问控制功能。以下选项中，对Windows操作系统访问控制实现方法的理解错误的是（） 分值1分

- A.ACL只能由管理员进行管理
- B.ACL是对象安全描述符的基本组成部分，它包括有权访问对象的用户和组的SID
- C.访问令牌存储着用户的SID、组信息和分配给用户的权限
- D.通过授权管理器，可以实现基于角色的访问控制

 回答正确

+1分

12.数据库的安全很复杂，往往需要考虑多种安全策略，才可以更好地保护数据库的安全。以下关于数据库常用的安全策略理解不正确的是（） 分值1分

- A.最小特权原则，是让用户可以合法的存取或修改数据库的前提下，分配最小的特权，使得这些信息恰好能够完成用户的工作
- B.最大共享策略，在保证数据库的完整性、保密性和可用性的前提下，最大程度地共享数据库中的信息
- C.粒度最小策略，将数据库中的数据项进行划分，粒度越小，安全级别越高，在实际中需要选择最小粒度
- D.按内容存取控制策略，不同权限的用户访问数据库的不同部分

 回答正确

+1分

13.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.信息处理实施的授权过程、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

14.与PDR模型相比，P2DR模型则更强调（），既强调系统安全的（），并且以安全检测、（）和自适应填充“安全间隙”为循环来提高（） 分值1分

- A.漏铜检测；控制和对抗；动态性；网络安全
- B.动态性；控制和对抗；漏洞监测；网络安全
- C.控制和对抗；漏洞监测；动态性；网络安全
- D.控制和对抗；动态性；漏洞监测；网络安全

 回答正确

+1分

15.老王是一名企业信息化负责人，由于企业员工在浏览网页时总导致病毒感染系统，为了解决这一问题，老王要求信息安全部员给出解决措施，信息安全部员给出了四条措施建

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

议，，老王根据多年的信息安全管理经验，认为其中一条不太适合推广，你认为是哪条措施（） 分值1分

- A.采购防病毒网关并部署在企业互联网出口中，实现对所有预览网页进行检测，阻止网页中的病毒进入网页
- B.采购并统一部署企业防病毒软件，信息化管理部门统一进行病毒库升级，确保每台计算机都具备有效的病毒检测和查杀能力
- C.制定制度禁止使用微软的IE浏览器上网，统一要求使用Chrome浏览器
- D.组织对员工进行一次上网行为安全培训，提高企业员工在互联网浏览时的安全意识。

 回答正确

+1分

16.你是单位安全主管，由于微软刚发布了数个系统漏补丁，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户端尽快安装补丁
- 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险，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，由终端自行升级。

 回答正确

+1分

17.关于对信息安全事件进行分类分级管理的原因描述不正确的是（） 分值1分

- A.信息安全事件的种类很多，严重程度也不尽相同，其响应和处理方式也应各不相同
- B.对信息安全事件进行分类和分级管理，是有效防范和响应信息安全事件的基础
- C.能够使事前准备、事中应对和事后处理的各项相关工作更具针对性和有效性
- D.我国早期的计算机安全实践的应急响应工作主要括计算机病毒防范和“千年虫”问题的解决，关于网络安全应急响应的起步最早

 回答正确

+1分

18.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定的，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

19.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.基于战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，有助于一个组在事件发生时阻由混的发生成是在混乱状态中迅速该复控制，将损失和负面影响降至最低

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- 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象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
- D.一种被广为接受的成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，这6个阶的响应方法一定确保事件处理的成功

 回答正确

+1分

20.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。一次增训的时候，小李主要负责培训讲解风险评估方法，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，因此更具客观性
- D.定量风险分新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

21.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。当检测统到来自内外网络对防火墙的抗攻击行为，会及时响应，并通知防火墙实时阻断攻击源，从而进一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

22.Kerberos协议是一种集中访问控制协议，它能在复杂的网络环境中，为用户提供安全的单点登录服务，单点登录是指用户在网络中进行一次身份认证，便可以访问其授权的所有网络资源，而不再需要其他的身份认证过程，实质是消息M在多个应用系统之间的传递或共享。其中，消息M是指以下选项中的（） 分值1分

- A.安全凭证
- B.用户名
- C.加密密钥
- D.会话密钥

 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**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

23.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
- 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

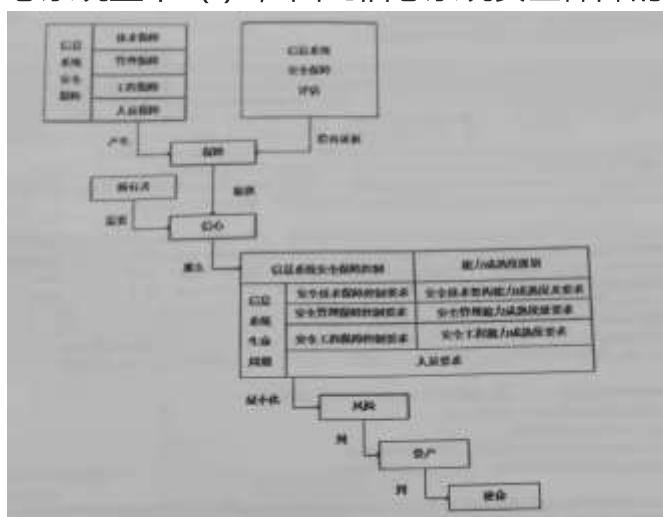
24.有关能力成熟度模型(CMM),错误的理解是（） 分值1分

- A.CMM的基本思想是，因为问题是由于技术落后引起的，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的思想来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，是一种面向工程过程的方法
- 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的产品”

回答正确

+1分

25.信息系统安全保障评估概念和关系如图所示，信息系统安全保障评估，就是在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估。通过信息系统安全保障评估所搜集的（）。向信息系统的所有相关方提供信息系统的（）能够实现其安全保障策略，能够将其所面临的风险降低到其可接受的程度的主观信心。信息系统安全保障评估的评估对象是（），信息系统安全保障是一个动态持续的过程，涉及信息系统整个（），因此信息系统安全保障的评估也应该提供一种（）的信心。（）



分值1分

- A.安全保障工作:客观证据:信息系统:生命周期:动态持续

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- B.客观证据:安全保障工作:信息系统:生命周期:动态持续
- C.客观证据, 安全保障工作:生命周期:信息系统:动态持续
- D.客观证据:安全保障工作;动态持续;信息系统:生命周期

 回答正确

+1分

26.以下关于互联网协议安全(InternetProtocolSecurityIPsec)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.验证头协议(AuthenticationHead, AH)和IP封装安全载荷协议 (EncapsulatingSecurityPayload, 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

27.应急响应是信息安全事件管的重要内容, 基于应急响应工作的特点和事件的不规性, 事先制定出事件响应方法和过程, 有助于一个组在事件发生时阻止混乱状态态中迅速恢复控制, 将损降到最低。应急响应方法和过程并不是唯一, 一种被广为接受的应急响应方法是将应响应管理过程分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 ( ) 分值1分

- A.确定重要产和风险, 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.遇到遏制可能会因为事件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恢复步骤, 顺次恢复相关的系统

 回答正确

+1分

28.某社交网站的用户点击了该网站上的一个广告, 该广告含有一个跨站脚本, 会将他的浏览器定向到旅游网站, 旅游网站则获得了他的社交网络信息, 虽然该用户没有主动访问该旅游网站, 但旅游网站已经截获了他的社交网络信息(还有他的好友的信息), 于是犯罪分子便可以躲藏在社交网站的广告后面, 截获用户的个人信息了。这种向Web页面插入恶意html代码的攻击方式称为 ( ) 分值1分

- A.分布式拒绝服式攻击
- B.跨站脚本攻击
- C.SQL注入攻击
- D.缓冲区溢出攻击

 回答正确

+1分

29. 软件安全设计和开发中应考虑用户隐私保护, 以下关于用户隐私保护的说法哪个是错误的? ( ) 分值1分

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

加微信 : vic\_tom , 进cisp考证备考群 , 请务必备注 : 备考

- A.告诉用户需要收集什么数据及搜集到的数据会如何被使用
- B.当用户的数据由于某种原因要被使用时, 给用户选择是否允许
- C.用户提交的用户名和密码属于隐私数据, 其它都不是
- D.确保数据的使用符合国家、地方、行业的相关法律法规

 回答正确

+1分

30.关于信息安全管理, 下面理解片面的是 () 分值1分

- A.信息安全管理是组织整体管理的重要、固有组成部分, 它是组织实现其业务目标的重要保障
- B.信息安全管理是一个不断演进, 循环发展的动态过程, 不是一成不变的
- C.在信息安全建设中, 技术是基础, 管理是拔高, 既有效的管理依赖于良好的技术基础
- D.坚持管理与技术并重的原则, 是我国加强信息安全保障工作的主要原则之一。

 回答正确

+1分

31.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, 评估被利用和击发生的率, 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险, 它可能是故意的, 也可能不是故意的, 威胁就是漏洞

 回答正确

+1分

32.“统一威胁管理”是将防病毒、入侵检测和防火墙等安全需求统一管理, 目前市场上已经出现了多种此类安全设备, 这里“统一威胁管理”常常被简称为 () 分值1分

- A.UTM
- B.FW
- C.IDS
- D.SOC

 回答正确

+1分

33.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

加微信 : vic\_tom , 进cisp考证备考群 , 请务必备注 : 备考

D.6 回答正确

+1分

34.PKI的主要理论基础是（） 分值1分

- A.对称密码算法
- B.公钥密码算法
- C.量子密码
- D.摘要算法

 回答正确

+1分

35.某购物网站开发项目经过需求分析进入系统设计阶段，为了保证用户帐户的安全，项目开发人员决定用户登录时如果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，将暂时禁止登录该帐户，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.最少共享机制原则
- 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

36.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.ARPA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，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

37.小张新购入了一台安装了Windows操作系统的笔记本电脑，为了提升操作系统的安全性，小张在Window系统中的“本地安全策略”中，配置了四类安全策略：账号策略、本地策略、公钥策略和IP安全策略。那么该操作属于操作系统安全配置内容中的（） 分值1分

- A.关闭不必要的服务
- B.制定操作系统安全策略
- C.关闭不必要的端口
- D.开启审核策略

 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

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

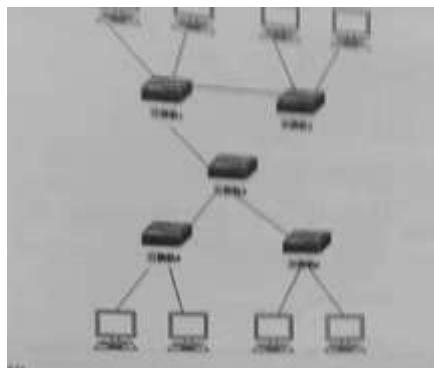
38.为保障信息系统安全，某经商公司服务系统的公司准备并编制一份针对性的信息安全保障方案，并将编制任务交给了小王，为此，小王决定首先编制出一份信息安全需求描述报告，关于此项工作，下面说法错误的是（） 分值1分

- A.信息安全需求报告应该根据公司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设计是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关于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要展开编写

 回答正确

+1分

39.某银行有5台交换机连接了大量交易机构的网络(如图所示)在基于以太网的通信中，计算机A需要与计算机B通信，A必须先广播“ARP请求信息”，获取计算机B的物理地址。每到月底时用户发现该银行网络服务速度极其缓慢，银行经调查后发现为了当其中一台交换机收到ARP请求后，会转发给接收端口以外的所有端口，ARP请求会被转发到网络中的所有客户机上，为降低网络的带宽消耗，将广播流限制在固定区域内，可以采用的技术是（） 分值1分



技术是（）

- A.VLAN划分
- B.动态分配地址
- C.为路由交换设备修改默认口令
- D.设立入侵防御系统

 回答正确

+1分

40.国家科学技术秘密的密级分为绝密级、机密级、秘密级，以下哪项属于绝密的描述（） 分值1分

- A.处于国际先进水平，并且有军事用途或者对经济建设具有重要影响的
- B.能够局部反应国家防御和治安实力的
- C.我国独有、不受自然条件因素制约、能体现民族特色的精华，并且社会或经济效益显著的传统工艺
- D.国际领先，并且对国防建设或者经济建设具有特别重大影响的

 回答正确

+1分

41.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人力资源安全方面实施常规控制，人力资源安全划分为3个控制阶段，不包括哪一项（） 分值1分

- A.任用之前

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

- B.任用中
- C.任用终止或变化
- D.任用公示

 回答正确

+1分

42.社会工程学定位在计算机信息安全工作链的一个最重要的环节，即“人”这个环节上，这些社会工程黑客在某黑客大会上成功收入世界五百强公司，其中一名自称为是CSO杂志做安全调查，半小时内，攻击者选择了在公司工作两个月安全工程部门的合约雇员，在询问关于工作满意度以及食堂食物质量问题后，雇员开始透露其他信息，包括，操作系统，服务包，杀毒软件，电子邮件及浏览器。为对执此类信息收集和分析，公司需要做的是（） 分值1分

- A.通过信息安全意识培训，使相关信息发布人员了解信息收集风险，发布信息采取最小化原则
- B.减少系统对外服务的端口数量，修改服务旗标
- C.关闭不必要的服务，部署防火墙，IDS等措施
- D.系统安全管理员使用漏铜扫描软件对系统进行安全审计

 回答正确

+1分

43.在软件保障成熟度模型（Software Assurance Maturity ModeSAMM）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组件的相关管理过程与活动

 回答正确

+1分

44.实体身份签别的样，且随着技术的进步鉴别方法的强度不断提高，常见的方法有利用口令鉴别、令牌鉴别、指纹鉴别等，小王在登陆某移动支付平台时，首先需要通过指纹对用户身份进行鉴别。通过鉴别后，他才能作为合法用户使用自己的户进行支付、转账等操作。这种鉴别方法属于下列选项中的（） 分值1分

- A.实体所知的鉴别方法
- B.实体所有的鉴别方法
- C.实体特征的鉴别方法
- D.实体所见的鉴别方法

 回答正确

+1分

45.在某信息系统的建设中，用户登录过程是这样的(1)用户通过HTTP协议访问信息系统，(2)用户在登录页，面输入用户名和口令:(3)信息系统在服务器端检查用户名和密码的正确性，如果正确，则鉴别完成，可以看出，这个鉴别过程属于（） 分值1分

- A.单向鉴别

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

- B. 双向鉴别
- C. 三向鉴别
- D. 第三方鉴别

 回答正确

+1分

46. 自主访问控制模型（DAC）的访问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柜库，通常使用由客体指向的链表来储存数据，下面选项中正确的是（ ） 分值1分

- A. ACL是Bell-Lapadula模式的一种具体实现
- 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比较简单

 回答正确

+1分

47. 某单位在实施信息安全风险评估后，形成了若干文档，下面（ ）中的档不应属于风险评估中“风险评估准备”阶段输出的文档。 （ ） 分值1分

- A. 《风险评估工作计划》，主要包括本次风险评估的目的意义、范围、目标、组织结构，角色及职责，经费预算和进度安排内容
- B. 《风险评估方法和工具表》，主要包括拟用的风险评估方法和测试估工等内容
- C. 《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
- D. 《风险评估准则要求》，主要报告风险评估风险评估参考标准，采用的风险分析方法，风险计算方法，资产分类标准，要产分类准则等内容

 回答正确

+1分

48. 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，而依赖与秘钥。
- 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秘钥，不影响安全性
- C. 密钥管理要在安全策略的指导下处理秘钥生命周期的整个过程，包括产生，存储、备份、分配、更新、等
- D. 在保密通信过程中，通信双方也可利用Diffie-Hellman协议协商出会话秘钥进行保密通信。

 回答正确

+1分

49. 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的准备、以及在事件发生所采取的措施
- B. 应急响应方法，将应急响应管理过程分为遏制、根除、处置、快复、报告和跟踪6个阶段

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- C.对信息安全事件的分级主要参考信息系统的要程度、系统损失和社会影响三要素事件划分为4个级别，特别重大事件（I级），重大事件（II级），较大事件(III级)和一般事件(IV级)
- D.根据信息安全事件的分级参考要素，可将信息安全

 回答正确

+1分

50.一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，一个学校的务系统中、教师够录生的考试绩，学生只能查看自己的分数，而学校教务门的管理人员能够对课程信息、学生的选课等内容进行修改，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用

 回答正确

+1分

51.某单位门户网站开发完成后，测试人员使用模糊测试进行安全性测试，以下关于模糊测试过程的说法正确的是：（） 分值1分

- A.模拟正常用户输入行为，生成大量数据包作为测试用例
- B.数据处理点，数据通道的入口点和可信边界点往往不是测试对象
- C.监测和记录输入数据后程序正常运行的情况
- D.深入分析网站测试过程中产生崩溃或异常的原因，必要时需要测试人员手工重现并分析

 回答正确

+1分

52.小王学习了灾难备份的有关知识，了解到常用的数据备份方式包括完全备份、增量备份、差量备份，为了巩固所学知识，小王对这三种备份方式进行了对比，其中在数据恢复速度方面三种备份方式由快到慢的顺序是（） 分值1分

- A.完全备份、增量备份、差异备份
- B.完全备份、差异备份、增量备份
- C.增量备份、差异备份、完全备份
- D.差异备份、增量备份、完全备份

 回答正确

+1分

53.在一个使用Chinese Wall模型建立访问控制的信息系统中，数据W和数据X在一个兴趣冲突，数据Y和Z在另一个信息兴趣冲突域中，那么可以确定一个新注册的用户

（） 分值1分

- A.只有访问了W之后，才可以访问X
- B.只有访问了W之后，才可以访问Y和Z中的一个
- C.无论是否访问W，都只能访问Y和Z中的一个

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- D.无论是否访问W,都不能访问Y或Z

回答正确

+1分

54.关于我国信息安全保障的基本原则，下列说法中不正确的是（） 分值1分

- A.要与国际接轨，积极吸收国外先进经验并加强合作，遵循国际标准和通行做法，坚持管理与技术
- B.信息化发展和信息安全不是矛盾的关系，不能牺牲一方以保证另一方
- C.在信息安全保障建设的各项工作中，既要统筹规划，又要突出重点
- D.在国家信息安全保障工作中，要充分发挥国家、企业和个人的积极性，不能忽视任何一方的作用

回答正确

+1分

55.小张是一名CISP人员。某天他听到小李说某电商平台在“双十一”节期间某款平板电脑如果输入1111，购买产品的单价就会变为1元。请问以下哪项行为符合作为CISP的职业道德（） 分值1分

- A.按照小李的说法尝试，发现成功后立即付款购买
- B.在微博上将该信息发布
- C.对该电商平台进行一次渗透测试，查找所有可能的漏洞
- D.打电话或发邮件告知该电商平台存在错误

回答正确

+1分

56.社会工程学是（）与（）结合的学科，准确来说，它不是一门科学，因为它不能总是重复和成功，并且在信息充分多的情况下它会失效。基于系统、体系、协议等技术体系缺陷的（），随着时间流逝最终都会失效，因为系统的漏洞可以弥补，体系的缺陷可能随着技术的发展完善或替代。社会工程学利用的是人性的“弱点”，而人性是（），这使得它几乎可以说是永远有效的（） 分值1分

- A.网络安全；心理学；攻击方式；永恒存在的；攻击方式
- B.网络安全；攻击方式；心理学；永恒存在的；攻击方式
- C.网络安全；心理学；永恒存在的；攻击方式；攻击方式
- D.网络安全；攻击方式；心理学；攻击方式；永恒存在的

回答正确

+1分

57.一般地，IP分配会首先把整个网络根据地域、区域。每个子区域从它的上一级区域里获取IP地址段，这种分配方法为什么分配方法（） 分值1分

- A.自顶向下
- B.自下向上
- C.自左向右
- D.自右向左

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**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

58. 入侵检测系统 (Intrusion Detection System, IDS) 是用于发现并报告系统中未授权或违反安全策略行为的设备。在入侵检测中有这样一种方法，任何的正常行为都是有一定的规律的并且可以通过分析这些行为产生的日志信息（假定日志信息足够安全）总结出这些规律。而入侵和滥用行为则通常和正常的行为存在严重的差异，通过检查这些差异就可以检测这些入侵，请问该入侵检测方法为（） 分值1分

- A. 基于异常的入侵检测
- B. 基于误用的入侵检测
- C. 基于自治代理技术
- D. 自适应模型生成特性的入侵检测

 回答正确

+1分

59. CC标准是计算机安全认证的国际标准 (ISO/IEC15408) .CC标准中四个关键概念，分别为TOE、PP、ST、EAL，它们的含义分别是（） 分值1分

- A. 保护轮廓；安全目标；评估对象；评估保证级
- B. 保护轮廓；评估对象；评估保证级；安全目标
- C. 评估对象；保护轮廓；安全目标；评估保证级
- D. 评估对象；保护轮廓；评估保证级；安全目标

 回答正确

+1分

60. 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

61. 以下行为不属于违反国家保密规定的行为：（） 分值1分

- A. 将涉密计算机、涉密存储设备接入互联网及其他公共信息网络
- B. 通过普通邮政等无保密措施的渠道传递国家秘密载体
- C. 在私人交往中涉及国家秘密
- D. 以不正当手段获取商业秘密

 回答正确

+1分

62. 目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握能力和掌握资源分，这些威胁可以按照个人威胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是（） 分值1分

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- A.喜欢恶作剧、实现自我挑战的娱乐型黑客
- B.实施犯罪、获取非法经济利益网络犯罪团伙
- C.搜集政治、军事、经济等情报信息的情报机构
- D.巩固战略优势，执行军事任务、进行目标破坏的信息作战部队

 回答正确

+1分

63.信息安全事件的分类方法有很多种，依据GB/Z20986-2007《信息安全技术信息安全事件分类分级指南》，信息安全事件分7个基本类别，描述正确的是（） 分值1分

- A.有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。
- B.网络攻击事件、拒绝服务攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。
- C.网络攻击事件、网络钓鱼事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。
- D.网络攻击事件、网络扫描窃听事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。

 回答正确

+1分

64.关于源代码审核，下列说法正确的是（） 分值1分

- A.源代码审核往往需要大量的时间，采用人工审核费事费力，但可以通过多人并行审核来弥补这个缺点。
- B.源代码审核工具应当以检查源代码的功能是否完整、是否执行正确为主要功能。
- C.使用源代码审核工具自动化执行代码检查和分析，能够极大提高软件可靠性并节省软件开发和测试的成本，已经取代人工审核方式。
- D.源代码审核是指无需运行被测代码，仅对源代码检查分析，检测并报告源代码中可能隐藏的错误和缺陷。

 回答正确

+1分

65.国务院信息化工作办公室于2004年9月份下发了《关于做好重要信息系统灾难备份工作的通知》，该文件中指出了我国在灾备工作原则，下面哪项不属于该工作原则（） 分值1分

- A.统筹规划
- B.分级建设
- C.资源共享
- D.平战结合

 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**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

66.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

67.应用安全，一般是指保障应用程序使用过程和结果的安全。以下内容中不属于应用安全防护考虑的是 ( ) 分值1分

- A.身份鉴别，应用系统应对登录的用户进行身份鉴别，只有通过验证的用户才能访问应用系统资源
- B.安全标记，在应用系统层面对主体和客体进行标记，主体不能随意更改权限，增加访问控制的力度，限制非法访问
- C.剩余信息保护，应用系统应加强硬盘、内存或缓冲区中剩余信息的保护，防止存储在硬盘、内存或缓冲区中的信息被非授权的访问
- D.机房与设施安全，保证应用系统处于有一个安全的环境条件，包括机房环境、机房安全等级、机房的建造和机房的装修等

 回答正确

+1分

68.安全领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

69.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，自评估和检查评估互相结合、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

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

70.信息安全组织的管理涉及内部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.

回答正确

+1分

71.以下哪一项不是信息系统集成项目的特点：（） 分值1分

- A.信息系统集成项目要以满足客户和用户的需求为根本出发点
- B.系统集成就是选择最好的产品和技术，开发相应的软件和硬件，将其集成到信息系统的过程。
- C.信息系统集成项目的指导方法是“总体规划、分布实施”。
- D.信息系统集成包含技术，管理和商务等方面，是一项综合性的系统工程。

回答正确

+1分

72.关于SMTP和POP3的说法哪个是错误的是（） 分值1分

- A.是一种基于ASCII的编码请求/响应的模式的协议
- B.明文传输数据，因此存在数据泄露的可能
- C.缺乏严格的用户认证，因此导致了垃圾邮件问题
- D.协议过于简单，易用性更高，更容易实现远程管理邮件

回答正确

+1分

73.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

回答正确

+1分

74.风险计算原理可以用下面的范式形式化地加以说明：风险值=R(A,T,V)=R(L(T,V),F(Ia,Va))以下关于上式各项说明错误的是：（） 分值1分

- A.R表示安全风险计算函数，A表示资产，T表示威胁，V表示脆弱性
- B.L表示威胁利用资产脆弱性导致安全事件的可能性
- C.F表示安全事件发生后造成的损失
- D.Ia, Va分别表示安全事件作用全部资产的价值与其对应资产（应为脆弱性）的严重程度.

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**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

75.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。下面选项中属于使用基于实体特征的鉴别方法的是（） 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.通过扫描和识别用户的脸部信息来鉴别

 回答正确

+1分

76.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，它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

77.某网站为了开发的便利，使用SA连接接数据库，由于网站脚本中被发现存在SQL注入漏洞，导致攻击者利用内置存储过程XP\_cmdshell删除了系统中的一个重要文件，在进行问题分析时，作为安全专家，你应该指出该网站设计违反了以下哪项原则：

（） 分值1分

- A.权限分离原则
- B.最小特权原则
- C.保护最薄弱环节的原则
- D.纵深防御的原则

 回答正确

+1分

78.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年及以后的工作
- 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

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

79.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

- 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

80.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，包括生产、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

81.关于恶意代码的守护进程的功能，以下说法正确的是（） 分值1分

- A. 隐藏恶意代码
- B. 加大检测难度
- C. 传播恶意代码
- D. 监视恶意代码主体程序是否正常

 回答正确

+1分

82.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，这些标准可以依照等级保护工作的阶段分级。下面四个标准中，

（）规定了等级保护定级阶段的依据、对象、流程、方法及登记变更等内容：

（） 分值1分

- A. GB/T20271-2006《信息系统通用安全技术要求》
- B. GB/T《信息系统安全保护登记定级指南》
- C. GB/T《信息系统等级保护安全设计技术要求》
- D. GB/T《信息系统安全管理要求》

 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

83.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（security protocol），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

84.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，采用法律的手段制裁计算机犯罪，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.减低威胁能力，采取身份认证措施，从而抵制身份假冒这种威胁行为的能力
- D.减少脆弱性，及时给系统打补丁，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

85.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

86.信息安全标准化工作是我国信息安全保障工作的重要组成部分之一，也是政府进行宏观管理的重要依据，同时也是保护国家利益、促进产业发展的重要手段之一。关于我国信息安全标准化工作，下面选项中描述错误的是（） 分值1分

- A.我国是在国家质量监督检验检疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，下设有专业技术委员会。
- B.因事关国家安全利益，信息安全因此不能和国际标准相同，而是要通过本国组织和专家制定标准，确实有效地保护国家利益和安全

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- C. 我国归口信息安全方面标准的是“全国信息安全标准化技术委员会”，为加强相关工作，2016在其下设立“大数据安全特别工作组”
- D. 信息安全标准化工作是解决信息安全问题的重要技术支撑，其主要作用突出地体现在能够确保有关产品、设施的技术先进性、可靠性和一致性

 回答正确

+1分

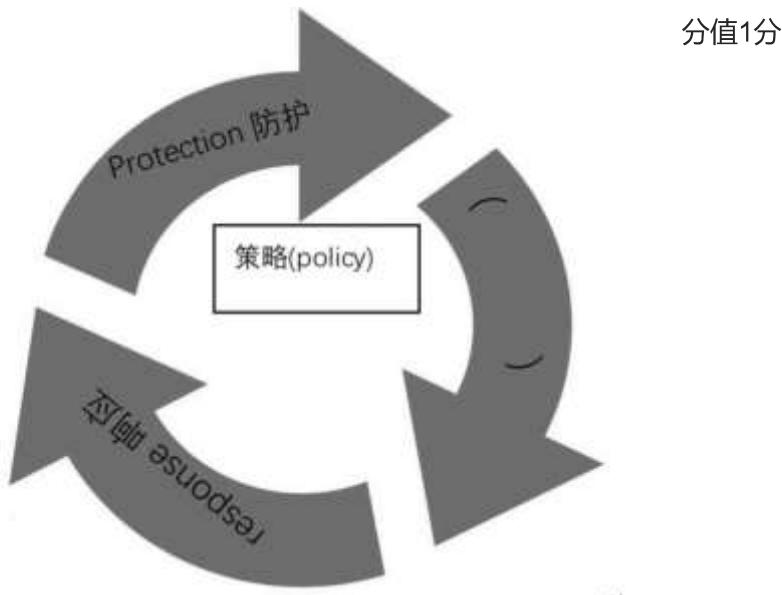
87. 系统工程的模型之一霍尔三维结构模型由时间维、逻辑维和知识维组成。有关此模型，错误的是（） 分值1分

- A. 霍尔三维结构体系形象地描述了系统工程研究的框架
- B. 时间维表示系统工程活动从开始到结束按时间顺序排列的全过程
- C. 逻辑维的七个步骤与时间维的七个阶段严格对应，即时间维第一阶段应执行逻辑维第一步骤的活动，时间维第二阶段应执行逻辑维第二步骤的活动
- D. 知识维列举可能需要运用的工程、医学、建筑、商业、法律、管理、社会科学和艺术等各种知识和技能

 回答正确

+1分

88. P2DR模型是一个用于描述网络动态安全的模型，这个模型经常使用图形的形式来形象表达，如下图所示：请问图中空白处应填写是（） 分值1分



分值1分

- A. 执行 (do)
- B. 检测 (detection)
- C. 数据 (data)
- D. 持续 (direction)

 回答正确

+1分

89. 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果的重要基础。按照规范的风险评估流程，下面哪个文档应当是风险要素识别阶段的输出成果（） 分值1分

- A. 《风险评估方案》

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

**加微信：vic\_tom，进cisp考证备考群，请务必备注：备考**

- B.《需要保护的资产清单》
- C.《风险计算报告》
- D.《风险程度等级列表》

 回答正确

+1分

90.某电子商务网站在开发设计时，使用了威胁建模方法来分析电子商务网站所面临的威胁。STRIDE是微软SDL中提出的威胁建模方法，将威胁分为6类，为每一类威胁提供了标准的消减措施，spoofing是STRIDE中欺骗类的威胁。以下威胁中哪个可以归入此类威胁（） 分值1分

- A.网站竞争对手可能雇佣攻击者实施DDOS攻击，降低网站访问速度；
- B.网站使用http协议进行浏览等操作，未对数据进行加密，可能导致用户传输信息泄露，例如购买的商品金额等；
- C.网站使用http协议进行浏览等操作，无法确认数据与用户发出的是否一致，可能数据被中途篡改
- D.网站使用用户名、密码进行登录验证，攻击者可能会利用弱口令或其他方式获得用户密码，以该用户身份登录修改用户订单等

 回答正确

+1分

91.一个密码系统至少由明文、密文、加密算法、解密算法和密钥五部分组成，而其安全性是由下列哪个选项决定的（） 分值1分

- A.加密算法
- B.解密算法
- C.加密和解密算法
- D.密钥

 回答正确

+1分

92.基于TCP的主机在进行一次TCP连接时需要进行三次握手。请求通信的主机A要与另一台主机B建立连接时，A需要先发一个SYN数据包向B主机提出连接要求，B收到后，回复一个ACK/SYN确认请求给A主机。然后A再次回应ACK数据包，确认连接请求。攻击通过伪造带有虚假源地址的SYN包给目标主机，使目标主机发送的ACK/SYN包得不到确认。一般情况下，目标主机会等一段时间后才会放弃这个连接等待，因此大量虚假SYN包同时发送到目标主机时，目标主机上就会有大量的连接请求等待确认，当这些未释放的连接请求数量超过目标主机的资源限制时，正常的连接请求就不能被目标主机接受。这种SYNFlood攻击属于（） 分值1分

- A.拒绝服务攻击
- B.分布式拒绝服务攻击
- C.缓冲区溢出攻击
- D.SQL注入攻击

 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**

93.某汽车保险公司有庞大的信贷数据,基于这些可信的不可篡改的数据,公司希望利用区块链的技术,根据预先定义好的规则和条款,自动控制保险的理赔。这一功能主要利用了的区块链的()技术特点 分值1分

- A.分布式账本
- B.非对称加密和授权技术
- C.共识机制
- D.智能合约

 回答正确

+1分

94.I Pv4协议在设计之初并没有过多地考虑安全问题,为了能够使网络方便地进行互联互通,仅仅依靠IP头部校验和字段来保证IP包的安全,因此IP包很容易被篡改,并重新计算校验和。IETF于1994年开始制定IPSec协议标准,其设计目标是在IPv4和IPv6环境中为网络层流量提供灵活、透明的安全服务保护TCP/IP通信免遭窃听和篡改,保证数据的完整性和机密性,有效抵御网络攻击,同时保持易用性,下列选项中说法错误的是() 分值1分

- A.对于IPv4,Ipsec是可选的,对于IPv6,Ipsec是强制实施的
- B.Ipsec协议提供对IP及其上层协议的保护
- C.Ipsec是一个单独的协议
- D.Ipsec安全协议给出了封装安全载荷和鉴别头两种通信保护机制

 回答正确

+1分

95.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,用来攻击基础设施
- C.指一类漏洞,即特别好被利用,一旦成功利用该类漏洞,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,但是还未公开、还不存在安全补丁的漏洞都是零日漏洞

 回答正确

+1分

96.有关项目管理,错误的理解是() 分值1分

- A.项目管理是一门关于项目资金、时间、人力等资源控制的管理学科
- B.项目管理是运用系统的观点、方法和理论,对项目涉及的全部工作进行有效地管理,不受项目资源的约束
- C.项目管理包括对项目范围、时间、成本、质量、人力资源、沟通、风险、采购、集成的管理
- D.项目管理是系统工程思想针对具体项目的实践应用

 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

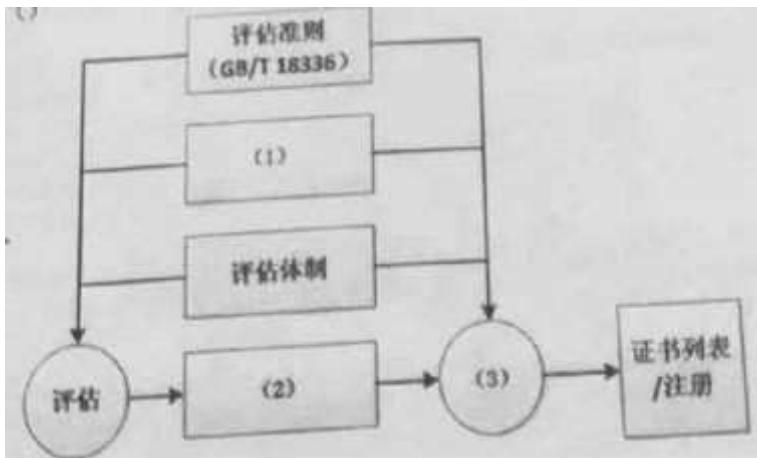
97.规范的实施流程和文档管理,是信息安全风险评估能否取得成果的重要基础。某单位在实施风险评估时,形成了《风险评估方案》并得到了管理决策层的认可。在风险评估实施的各个阶段中,该《风险评估方案》应是如下( )中的输出结果() 分值1分

- A.风险评估准备阶段
- B.风险要素识别阶段
- C.风险分析阶段
- D.风险结果判定阶段

回答正确

+1分

98.下图是使用CC标准进行信息安全评估的基本过程在图(1) - (3)处填入构成评估相关要素的主要因素,下列选项中正确的是()



分值1分

- A. (1) 评估方法学 (2) 最终评估结果 (3) 批准、认证
- B. (1) 评估方法学 (2) 认证过程 (3) 最终评估结果
- C. (1) 评估合理性 (2) 最终评估结果 (3) 批准、认证
- D. (1) 评估合理性 (2) 认证过程 (3) 最终评估结果

回答正确

+1分

99.Myers在1979年提出了一个重要观点, 使用人工和自动化的手段来运行或者测试某个系统的过程, 其目的在于是否满足规定的需求或是弄清预期结果与实际结果之间的差异, 那么他认为软件测试目的是() 分值1分

- A.证明程序正确
- B.验证程序无错误
- C.改正程序错误
- D.查找程序错误

回答正确

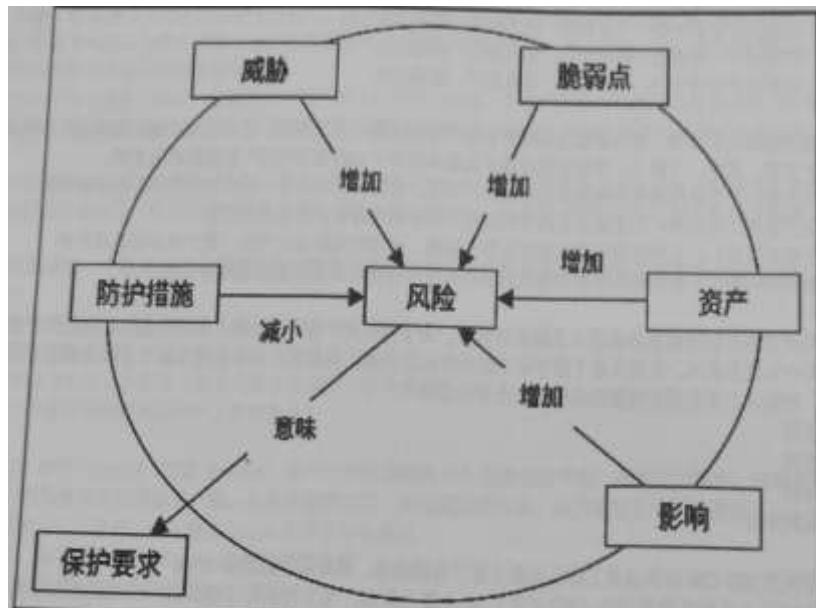
+1分

100.风险, 在GB/T22801中定义为事态的概率及其结果的组合。风险的目标可能有很多不同的方面, 如财务目标、健康和人身安全目标、信息安全目标和环境目标等;目标也可能有不同的级别, 如战略目标、组织目标、项目目标、产品目标和过程目标等。ISO/IE

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考  
C13335-1中揭示了风险各要素关系模型，如图所示。请结合此图，怎么才能降低风险对组织产生的影响？（）

分值1分



组织产生的影响？（）

- A.组织应该根据风险建立相应的保护要求，通过构架防护措施降低风险对组织产生的影响。
- B.加强防护措施，降低风险。
- C.减少威胁和脆弱点，降低风险。
- D.减少资产降低风险。

✓ 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  
<https://ks.wjx.top/wjx/join/completetmobile2.aspx?activityid=w305cds&joinactivity=114326341156&sojumpindex=243&tvd=ui%26Bkd7Q%2bk...>

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

1

填写表单

2

提交表单

3

提取福利



感谢您的耐心填写，为您准备了  
1份小礼物，待领取 >

去领取

-  邀您参与有奖调查 赚4元零钱
-  139\*\*\*\*5378 刚提现了10元零钱



问卷星 提供技术支持

举报

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

<https://ks.wjx.top/wjx/join/completetmobile2.aspx?activityid=w305cds&joinactivity=114326341156&sojumpindex=243&tvd=ui%26Bkd7Q%2bk...> 28/28