

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

## CISP练习题五

小胡

答题人

100

总分100

100

答对

共100题

答案解析 

全部题目 错题集

姓名：

小胡

一、单项选择题。（每题1分，共100题，合计100分）

1、小王是某大学计算机科学与技术专业的学生，最近因为生病缺席了几堂信息安全课程，这几次课的内容是自主访问控制与强制访问控制，为了赶上课程进度，他向同班的小李借来课堂笔记，进行自学。而小李在听课时由于经常走神，所以笔记中会出现一些错误。下列选项是小李笔记中关于强制访问控制模型的内容，其中出现错误的选项是（） 分值1分

- ☐ A、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
- ☐ B、安全属性是强制性的规定，它由安全管理员或操作系统根据限定的规则确定，不能随意修改
- ☐ C、系统通过比较客体主体的安全属性来决定主体是否可以访问客体
- ☒ D、它是一种对单个用户执行访问控制的过程和措施

 回答正确

+1分

2、信息安全是国家安全的重要组成部分，综合研究当前世界各国信息安全保障工作，下面总结错误的是（） 分值1分

- ☐ A、各国普遍将与国家安全、社会稳定和民生密切相关的关键基础设施作为信息安全保障的重点
- ☐ B、各国普遍重视战略规划工作，逐步发布网络安全战略、政策评估报告、推进计划等文件
- ☒ C、各国普遍加强国际交流与对话，均同意建立一致的安全保障系统，强化各国安全系统互通

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、各国普遍积极推动信息安全立法和标准规范建设，重视应急响应、安全监管和安全测评

✔ 回答正确

+1分

3、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（还有他的好友们的信息），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、分布式拒绝服务攻击

● 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

4、模糊测试，也称Fuzz测试，是一种通过提供非预期的输入并监视异常结果来发现软件故障的方法。下面描述正确的是（） 分值1分

● A、模糊测试本质上属于黑盒测试

○ B、模糊测试本质上属于白盒测试

○ C、模糊测试有时属于黑盒测试，有时属于白盒测试，取决于其使用的测试方法

○ D、模糊测试既不属于黑盒测试，也不属于白盒测试

✔ 回答正确

+1分

5、若一个组织声称自己的ISMS符合ISO/IEC 27001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

○ B、任用中

○ C、任用终止或变化

● D、任用公示

✔ 回答正确

+1分

6、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的攻击，以下做法无用的是（） 分值1分

○ A、不下载、不执行、不接收来历不明的软件和文件

○ 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、使用共享文件夹

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、安装反病毒软件和防火墙，安装专门的木马防范软件

☒ 回答正确

+1分

7、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安全事件后，工作人员应在3 小时内完整应急处理工作并恢复对外运行
- ☐ C、该信息系统发生重大安全事件后，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
- ☒ D、该信息系统发生重大安全事件后，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

8、Kerberos 协议是一种集中访问控制协议，他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

9、若一个组织声称自己的ISMS 符合ISO/IEC 27001 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，资产管理包括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、资产负责人
- ☐ 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

10、在使用系统安全工程-能力成熟模型(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

- ☐ A、如果该组织在执行某个特定的过程区域时具备了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 Area,PA)具备了定义标准过程”、“执行已定义的过程 两个公

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

共特征,则此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 Area PA))包含4 个基本实施(Base Parctices,BP)执行此PA 时执行了3个BP,则此过程区域能力成熟度级别为0 D、组织在不同的过程区域的能力成熟可能处于不同的级别上

✔ 回答正确

+1分

11、数据流图是用来表示系统的功能的工具,表示系统的逻辑模型,描述了数据流在系统中流动的情况;它是一种功能模型,是常用的进行软件需求分析的图形工具,其基本图形符号是 ( ) 分值1分

- A、输入、输出、外部实体和加工
- B、变换、加工、数据流和存储
- C、加工数据流、数据存储和外部实体
- D、变换、数据存储、加工和数据流

✔ 回答正确

+1分

12、把瀑布模型和专家系统结合在一起,在开发的各个阶段上都利用相应的专家系统来帮助软件人员完成开发工作。 分值1分

- A、原型模型
- B、螺旋模型
- C、基于知识的智能模型
- D、喷泉模型

✔ 回答正确

+1分

13、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

✔

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

回答正确

+1分

14、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，指在2002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，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、一类漏洞，刚被发现后立即被恶意利用的安全漏洞。一般来说，那些已经被别人发现，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

15、随着信息安全涉及的范围越来越广，各个组织对信息安全的需求越来越迫切，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

16、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科学
- ☒ B、项目管理是运用系统的观点、方法、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

17、开发软件所需高成本和产品的低质量之间有着尖锐的矛盾，这种现象称作（） 分值1分

- ☐ A、软件工程
- ☐ B、软件周期
- ☒ C、软件危机
- ☐ D、软件产生

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

✔ 回答正确

+1分

18、CB/T 20984-2007《信息安全技术信息安全义批详选规范》、对10个（）进行了定义阐述其相关关系，规定了（）的原理和（）规定了风险评估实施的7个阶段的具体方法和要求，规定了针对信息系统（）5个阶段风险评估的常见（），给出了风险评估的一般计算方法和相关工具建议。（） 分值1分

- ☒ A、风险要素；风险评估；实施流程；生命周期；工作形式
- ☐ B、风险要素；实施流程；风险评估；生命周期；工作形式C、
- ☐ C、风险要素；生命周期；风险评估；实施流程；工作形式D、
- ☐ D、风险要素；工作形式；风险评估；实施流程；生命周期

✔ 回答正确

+1分

19、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
- ☐ C、风险结果判定
- ☐ D、风险处理

✔ 回答正确

+1分

20、超文本传输协议(HyperText Transfer Protocol,HTTP)是互联网上广泛使用的一种网络协议，下面哪种协议基于HTTP 并结合SSL 协议，具备用户鉴别和通信数据加密等功能（） 分值1分

- ☐ A、HTTP1.0 协议
- ☐ B、HTTP1.1 协议
- ☒ C、HTTPS 协议
- ☐ D、HTTPD 协议

✔ 回答正确

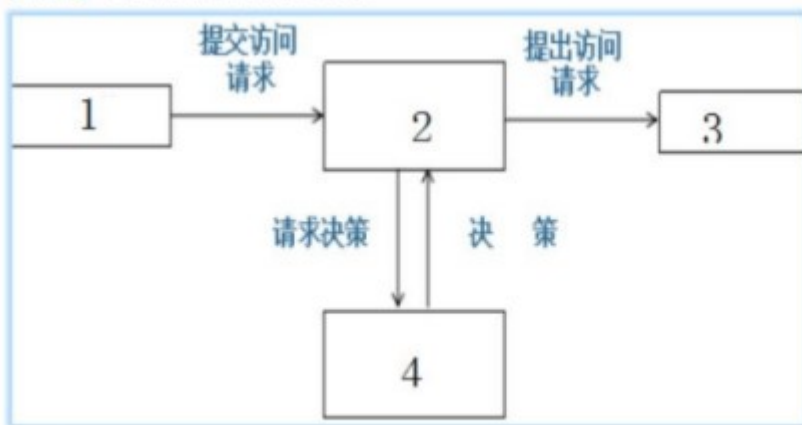
+1分

21、访问控制的实施一般包括两个步骤:首先要鉴别主体的合法身份，根据当前系统的访问控制规则授予用户相应的访问权限。在此过涉及主体、客体、访问控制实施部件和访问控制决策 部件之间的交互。下图所示的访问控制实施步骤中，标有数字的方框代表了主体、客体、访问控制实施部件和访问控制决策部件。下列选项中，标有数字1、2、3、4 的方框分别对应的实 体或部件正确的是（）

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

分值1分



(单选)

- ☐ A、主体、访问控制决策、客体、访问控制实施
- ☒ B、主体、访问控制实施，客体、访问控制决策
- ☐ C、客体、访问控制决策、主体、访问控制实施
- ☐ D、客体、访问控制实施、主体、访问控制决策

✔ 回答正确

+1分

22、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
- ☒ D、最小化反馈信息

✔ 回答正确

+1分

23、/etc/passwd 文件是UNIX/Linux 安全的关键文件之一。该文件用于用户登录时校验用户的登录名、加密的口令数据项、用户ID(UID)、默认的用户分组ID(GID)、用户信息、用户登录目录以及登录后使用的shell 程序。某黑客设法窃取了银行账户管理系统的passwd 文件后，发现每个用户的加密的口令数据项都显示为“X”。下列选项中，对此现象的解释正确的是（） 分值1分

- ☐ A.黑客窃取的passwd 文件是假的
- ☐ B.用户的登录口令经过不可逆的加密算法加密结果为“X”
- ☒ C.加密口令被转移到了另一个文件里
- ☐ D.这些账户都被禁用了

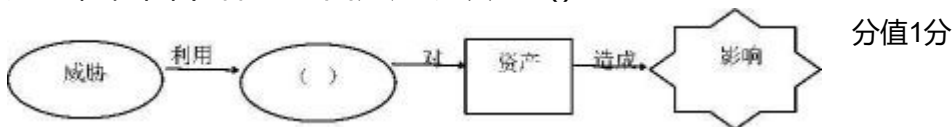
✔ 回答正确

+1分

24、陈工学习了信息安全风险的有关知识，了解到信息安全风险的构成过程，包括五个方面:起源、方式、途径、受体和后果。他画了下面这张图来描述信息安全风险的构

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：备考过程，图中括号空白处应该填写（）



- ☐ A、信息载体
- ☐ B、措施
- ☒ C、脆弱性

✔ 回答正确

+1分

25、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个阶段
- ☒ D、一种校广为接受的应色的应方法是将应色响应管理过程分为准备检刻、遏制、根除、恢复和跟踪总结6个阶段，这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

26、某单位计划在今年开发一套办公自动化(OA)系统，将集团公司各地的机构通过互联网进行协同办公在OA系统的设计方案评审会上，提出了不少安全开发的建议，作为安全专家，请指出大家提出的建议中不太合适的一条？（） 分值1分

- ☐ A对软件开发商提出安全相关要求,确保软件开发商对安全足够的重视，投入资源解决软件安全问题
- ☐ B、要求软件开发人员进行安全开发培训，使开发人员掌握基本软件安全开发知
- ☒ C、感求软件开发商使用Java 而不是ASP 作为开发语言，避免产生SQL 注入漏洞
- ☐ D、要求软件开发商格式，并在使用前对输入数据江软件进行模块化设计进行校验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

✔ 回答正确

+1分

27、以下哪项制度或标准被作为我国的一项基础制度加以推行，并且有一定强制性，其实施的主要目标是有效地提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全（） 分值1分

- ☐ A、信息安全管理体系统(ISMS)
- ☒ B、信息安全等级保护
- ☐ C、NIST SP800
- ☐ D、ISO 27000 系列

✔ 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

28、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)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 主体可以接收客体的信息和数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. 对目录的访问权限可分为读、写

✓ 回答正确

+1分

29、根据Bell-LaPadula 模型安全策略，下图中写和读操作正确的是 ( )

分值1分



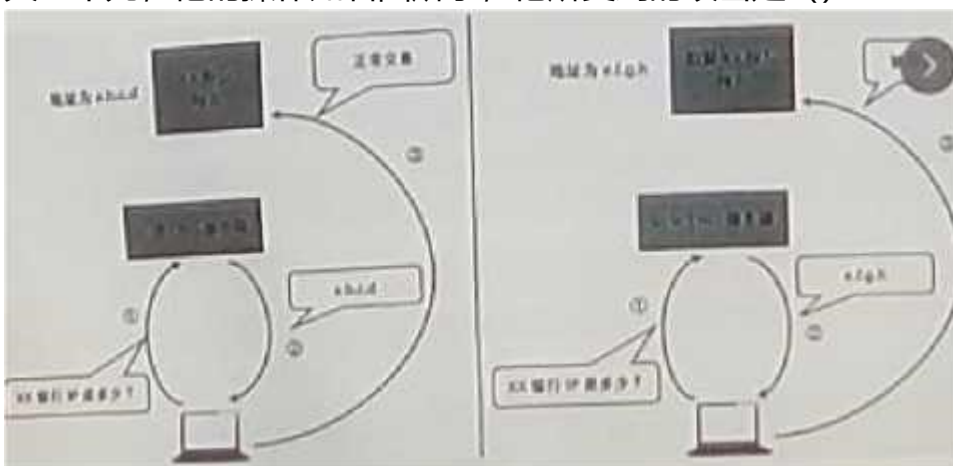
- ☐ A. 可写可读
- ☐ B. 可读不可写
- ☐ C. 可写不可读
- ☒ D. 不可读不可写

✓ 回答正确

+1分

30、小李在上网时不小心点开了假冒某银行的钓鱼网站，误输入了银行账号与密码损失上千元，他的操作如右图所示，他所受到的攻击是 ( )

分值1分



- ☐ A. ARP 欺骗
- ☒ B. DNS 欺骗
- ☐ C. IP 欺骗
- ☐ D. TCP 会话

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

✔ 回答正确

+1分

31、随着“互联网+”概念的普及，越来越多的新兴住宅小区引入了“智能楼宇”的理念，某物业为提供高档次的服务，防止网络主线路出现故障，保证小区内网络服务的可用、稳定、高效，计划通过网络冗余配置确保“智能楼宇”系统的正常运转，下列选项中不属于冗余配置的是（） 分值1分

- ☐ A、接入互联网时，同时采用不同电信运营商线路，相互备份且互不影响
- ☐ B、核心层、汇聚层的设备和重要的接入层设备均应双机热备、
- ☒ C、规划网络IP 地址，制定网络IP 地址分配策略
- ☐ D、保证网络带宽和网络设备的业务处理能力具备冗余空间，满足业务高峰期和业务发展需要

✔ 回答正确

+1分

32、根据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，按照要向公安机关备案即可，可以不需向上级或主管部门来测评和检查，此类信息系统应属于（） 分值1分

- ☐ A、零级系统
- ☐ B、一级系统
- ☒ C、二级系统
- ☐ D、三级系统

✔ 回答正确

+1分

33、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

34、20 世纪20 年代，德国发明家亚瑟·谢尔比乌斯(Auntur scherbius)和理查德·里特(Richard Ritter)发明了ENIGMA 密码机，看密码学发展历史阶段划分，这个阶段属于（） 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.古典密码阶段;这一阶段的密码专家常常靠直觉和技巧来设计密码,而不是推理和证明.常用的密码运算方法包括替代方法和置换方法。
- B.近代密码发展阶段。这一阶段开始使用机械代替手工计算，形成了机械式密码设备和更进一步的机电密码设备
- C.现代密码学的早起发展阶段。这一阶段以香农的论文“保密系统的通信理论”(the communication theory of secret systems )为理论基础，开始了对密码学的科学探索。
- D.现代密码学的近期发展阶段。这一阶段以公钥密码思想为标志，引发了密码学历史上的革命性的变革，同时，众多的密码算法开始应用于非机密单位和商业场合。

✔ 回答正确

+1分

35、某软件在设计时，有三种用户访问模式，分别是仅管理员可访问，所有合法用户可访问和允许匿名访问请问采用这三种访问模式时，攻击面最高的是（） 分值1分

- A、仅管理员可访问
- B、所有合法用户可访问
- C、允许匿名访问
- D、三种方式一样

✔ 回答正确

+1分

36、某单位开发了个面向互联网提供服务的应用网站，该单位委托软件测评机构对软件进行了源代码分析、模糊测试等软件安全性测试，在应用上线前，项目经理提出了还需要对应用网站进行一次渗透测试，作为安全主管，你需要提出渗透性测试相比源代码测试、模糊测试的优势给领导做决策，以下哪条是渗透性测试的优势？（） 分值1分

- A、渗透测试以攻击者的思维模拟真实攻击，能发现如配置错等运行维护所产生的漏洞
- B、渗透测试是用软件代替人工的一种测试方法，因此测试效更高
- C、渗透测试使用人工进行测试，不依赖软件，因此测试更准洞更多酒渗透测试中必须要查
- D、渗透测试必须查看软件源代码，因此测试中发现的漏洞更多

✔ 回答正确

+1分

37、某单位开发了一个面向互联网提供服务的应用网站，该单位委托软件测评机构对软件进行了源代码分析、模糊测试等软件安全性测试，在应用上线前，项目经理提出了还需要对应用网站进行一次渗透测试，作为安全主管，你需要提出渗透性测试相比源代码测试、模糊测试的优势给领导做决策，以下哪条是渗透性测试的优势？（） 分值1分

- A、渗透测试以攻击者的思维模拟真实攻击，能发现如配置错误等运行维护所产生的漏洞
- B、渗透测试是用软件代替人工的一种测试方法，因此测试效率更高
- C、渗透测试使用人工进行测试，不依赖软件，因此测试更准确
- D、渗透测试中必须要查看软件源代码，因此测试中发现的漏洞更多

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

✔ 回答正确

+1分

38、国家科学技术秘密的密级分为绝密级、机密级、密级，以下哪块属于绝密级的描述？（） 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、能够局部及应国家防制和治安实力的
- ☐ C、我国独有.不要自己条件因素制约.能体现民族特色的精华,并且社会效益或者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

39、根据《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》的规定，以下正确的是：（） 分值1分

- ☐ A.涉密信息系统的风险评估应按照《信息安全等级保护管理办法》等国家有关保密规定和标准进行
- ☐ B.非涉密信息系统的风险评估应按照《非涉及国家秘密的信息系统分级保护管理办法》等有关要求进行
- ☒ C.可委托同一专业机构完成等级测评的风险评估工作，并形成等级测评报告和风险评估报告
- ☐ D.此通知不要求将“信息安全风险评估作为电子政务项目验收的重要内容

✔ 回答正确

+1分

40、随着金融电子化的发展，全球金融通信网络已出具规模。某金融单位组建的计算机通信网络覆盖全国，有力的促进了该企业各种金融业务的发展。然而网络技术的普及、网络规模规模的延伸，开始逐步让该企业对网络安全提出了更高的要求。为了进一步促进金融电子化的建设，保障金融网络安全运行，该企业经过前期充分的调研分析与论证，实施了防火墙/VPN 系统建设项目。防火墙不能实现的安全功能是（）。 分值1分

- ☐ A、对出入网络的访问行为进行管理和控制
- ☐ B、过滤出入网络的数据，强化安全策略
- ☐ C、隐藏内部网络细节
- ☒ D、评估系统关键资源和数据完整性，识别已知的攻击行为

✔ 回答正确

+1分

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

- ☐ A、设计了三层WEB 架构，但是软件存在SQL 注入漏洞，导致被黑客攻击后能直接访问数据库
- ☐ B、使用C 语言开发时，采用了一些存在安全问题的字符串处理函数，导致存在缓冲区溢出漏洞
- ☒ 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

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、使用了符合要求的密码算法，但在使用算法接口时，没有按照要求生成密钥，导致黑客攻击后能破解并得到明文数据

✔ 回答正确

+1分

42、GB/T18336 的最低级别是 ( ) 分值1分

- A. ELA1
- B. ELA3
- C. ELA5
- D. ELA7

✔ 回答正确

+1分

43、在信息安全管理体的实施过程中，管理者的作用对于信息安全管理体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

44、鉴别是用户进入系统的第一道安全防线。用户登录系统时，和密码就是对用户身份进行鉴别。鉴别通过，即可以实现两的连接。例如，一个用户被服务器鉴别通过后，则被服务器用户，才可以进行后续访问。鉴别是对信息的一项安全属性该属性属于下列选项中的 ( ) 分值1分

- A、保密性
- B、可用性
- C、真实性
- D、完整性

✔ 回答正确

+1分

45、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，请问以下哪一项工作不能降低该系统的受攻击面： ( ) 分值1分

- A.分析系统功能的重要性
- B.分析从哪里可以访问这些功能
- C.采取合理措施降低特权

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.分析系统应满足的性能要求

✔ 回答正确

+1分

46、小李和小刘需要为公司新建的信息管理系统设计访问控制方法，他们在讨论中针对采用自主访问控制还是强制访问控制产生了分歧。小李认为应该采用自主访问控制的方法，他的观点主要有：(1)自主访问控制可为用户提供灵活、可调整的安全策略，具有较好的易用性和可扩展性；(2)自主访问控制可以抵御木马程序的攻击。小刘认为应该采用强制访问控制的方法，他的观点主要有：(3)强制访问控制中，用户不能通过运行程序来改变他自己及任何客体的安全属性，因为安全性较高；(4)强制访问控制能够保护敏感信息。请问以上四种观点中，正确的是 ( ) 分值1分

- A 观点(1)，因为自主访问控制的安全策略是固定的，主体的反问权限不能改变
- B 观点(2)，因为在自主访问控制中，操作系统无法区分对文件的访问权限是由合法用户修改，还是由恶意攻击的程序修改的
- C 观点(3)，因为在强制访问控制中，安全级别最高的用户可以修改安全属性
- D 观点(4)，因为在强制访问控制中，用户可能无意中泄漏机密信息

✔ 回答正确

+1分

47、在国家标准《信息系统安全保障评估框架第部分：简介和一般模型》(GB/T20274.1—2006)中描述了信息系统安全保障模型，下面对这个模型理解错误的是 ( ) 分值1分

- A、该模型强调保护信息系统所创建、传输、存储和处理信息的保密性、完整性和可用性等安全特征不被破坏，从而达到实现组织机构使命的目的
- B、该模型是一个强调持续发的动态安全模型即信息系统安全保障应该贯穿于整个信息系统生命周期的全过程
- C、该模型强调综合保障的观念，即信息系统的安全保障是通过综合技术、管理、工程和人员的安全保障来实施和实现信息系统的安全保障目标
- D、模型将风险和策略作为信息系统安全保障的基础和核心，基于IATF 模型改进，在其基础上增加了人员要素，强调信息安全的自主性

✔ 回答正确

+1分

48、出现错误。下列选项中，对图中出现的错误描述正确的是 ( )



分值1分

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

- ☐ A.步骤1 和2 发生错误，应该向本地AS 请求并获得远程TGT
- ☒ B.步骤3 和4 发生错误，应该本地TGS 请求并获得远程TGT
- ☐ C.步骤5 和6 发生错误，应该向远程AS 请求并获得远程TGT D、
- ☐ D.步骤5 和 6 发生错误，应该向远程TGS 请求并获得远程

✔ 回答正确

+1分

49、TCP/IP 协议Internet模型是Internet 构成的基础，TCP/IP 通常被认为是一个N 层协议，每一层都使用它的下一层所提供的网络服务来完成自己的功能，这里N 应等于（）。 分值1分

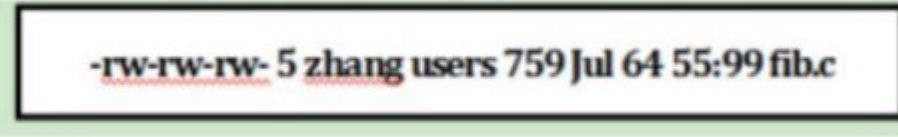
- ☒ A、 4
- ☐ B、 5
- ☐ C、 6
- ☐ D、 7

✔ 回答正确

+1分

50、Linux 系统的安全设置中，对文件的权限操作是一项关键操作。通过对文件权限的设置，能够保障不同用户的个人隐私和系统安全。文具fib.c 的文件属性信息如下图所示，小张 想要修改其文件权限，为文件属主增加执行权限，并删除组外其他用户的写权限，那么以下操作中正确的是（）

分值1分



```
-rw-rw-rw- 5 zhang users 759 Jul 64 55:99 fib.c
```

- ☐ A、 #chmod u+x,a-w fib.C
- ☐ B、 #chmod ug+x,o-w fib. C
- ☒ C、 #chmod 764 fib.c
- ☐ D、 # chmod467fib.C

✔ 回答正确

+1分

51、在工程实施阶段，以下哪一项不属于监理机构的监理重点： 分值1分

- ☐ A、督促承建单位严格按照经审批的实施方案进行施工
- ☐ B、 审查承建单位施工人员的身份与资格
- ☒ C、 部署工程实施人员安全管理措施
- ☐ D、 督促承建单位严格遵守业主单位相关安全管理规定

✔ 回答正确

+1分

52、微软提出了striderrepudiation（抵赖）的缩写R,关于此项安全要求，下面说法错误的是（） 分值1分

- ☐ A.某用户在登录系统并下载数据后，却声称“我没有下载过数据”，软件系统中的这种威胁属于R威胁

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.某用户在网络通信中传输完数据后，却声称“这些数据不是我传输的”，软件系统中的这种威胁属于R 威胁
- ☐ C、对于R 威胁，可以选择使用如强认证、数字签名，安全审计等技术措施来解决
- ☒ D、对于R 威胁，可以选择使用如隐私保护、过滤、流量控制等技术措施来解决

✔ 回答正确

+1分

53、风险分析是风险评估工作中的一个重要内容，GB/T20984-2007 在资料性附录中给出了一种矩阵法来计算信息安全风险大小，其中风险计算矩阵如下图所示，请为途

安全事件发生可能性

	1	2	3	4	5
1	3	6	9	12	16
2	5	8	11	15	18
3	6	9	13	17	21
4	7	11	16	20	23
5	9	14	20	23	25

分值1分

中括号空白 处选择合适的内容 ( )

- ☐ A、安全资产价值大小等级
- ☐ B、脆弱性严重程度等级
- ☐ C、安全风险隐患严重等级
- ☒ D 安全事件造成损失大小

✔ 回答正确

+1分

54、Ipsec (IP Security) 协议标准的设计目标是在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下面 选项中哪项描述是错误的 ( ) 分值1分

- ☒ A、IPSec 协议不支持使用数字证书
- ☐ B、IPSec 协议对于IPv4 和IPv6 网络都是适用的
- ☐ C、IPSec 有两种工作模式：传输模式和隧道模式
- ☐ D、IPSec 协议包括封装安全载荷 (ESP) 和鉴别头 (AH) 两种通信保护机制

✔ 回答正确

+1分

55、某电子商务网站架构设计时，为了避免数据误操作，在管理员进行订单删除时，需要由审核员进行审核后该操作才能生效，这种设计是遵循了以下哪个原则： ( ) 分值1分

- ☒ A、权限分离原则
- ☐ B、最小特权原则
- ☐ C、保护XXX 环节的原则
- ☐ D、纵深防御的原则

✔ 回答正确

+1分

56、安全漏洞产生的原因不包括以下哪一点 ( ) 分值1分

- ☐ A.软件系统代码的复杂性

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. 软件系统市场出现的信息不对称现象
- ☐ C. 复杂异构的网络环境
- ☒ D. 攻击者的恶意利用

✔ 回答正确

+1分

57、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(选择人居多)
- ☐ 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

58、小李是某公司的系统规划师，某天他针对公司信息系统的现状，绘制了一张系统安全建设规划图，如下图所示，请问这个图形是依据下面哪个模型来绘制的 ( )



- ☐ A、 PDR
- ☒ B、 PPDR
- ☐ C、 PDCA
- ☐ D、 IATF

✔ 回答正确

+1分

59、某攻击者想通过远程控制软件潜伏在某监控方的Unix 系统的计算机中，如果攻击者打算长时间地远程监控某服务器上的存储的敏感数据，必须要能够清除在监控方计算机中存在的系统日志。否则当监控方查看自己的系统日志的时候，就会发现被监控以及访问的痕迹。不属于清除痕迹的方法是 ( ) 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、窃取root 权限修改wtmp/wtmpxutmpx 和FQlastlog 三个主要日志文件
- ☐ B、采用干扰手段影响系统防火墙的审计功能
- ☒ C、保留攻击时产生的临时文件
- ☐ D、修改登录日志，伪造成功的登录日志，增加审计难度

✔ 回答正确

+1分

60、某公司拟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 公司为承建单位并选择了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A 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
- ☐ B. 质量控制计划
- ☐ C. 评审报告
- ☒ D. 需求说明书

✔ 回答正确

+1分

61、以下SQL 语句建立的数据库对象是：（）◆ Create View Patients ForDocotors A s ◆ Select Patient ◆ FROM Patient, Docotor ◆ Where docotorID= 123 分值1分

- ☐ A. 表
- ☒ B. 视图

✔ 回答正确

+1分

62、在某信息系统的设计中，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
- ☐ B、双向鉴别
- ☐ C、三向鉴别
- ☐ D、第三方鉴别

✔ 回答正确

+1分

63、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管
- ☒ 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

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

✔ 回答正确

+1分

64、某银行有5 台交换机连接了大量交易机构的网络，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其他端口， 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

- ☒ 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

65、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

- ☐ A.保障和促进信息化发展
- ☐ B.维护企业和公民的合法权益
- ☒ 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

66、某公司中标了某项软件开发项目后，在公司内部研讨项目任务时，项目组认为之前在VPN 技术方面积累不够，导致在该项目中难以及时完成VPN 功能模块，为解决该问题，公司高层决定接受该项目任务，同时将该VPN 功能模块以合同形式委托另外一家安全公司完成，要求其在指定时间内按照任务需求书完成工作，否则承担相应责任。在该案例中公司高层采用 哪种风险处理方式（） 分值1分

- ☐ A、风险降
- ☐ B、风险规避
- ☒ C、风险转移
- ☐ D、风险接受

✔ 回答正确

+1分

67、在工程实施阶段，监理单位依据承建合同、安全设计方案、实施方案、实施记录、国家或地方相关标准和技术指导文件，对信息化工程进行安全检查，以验证项目是否实现了项目设 计目标和安全等级要求。（） 分值1分

- ☐ A、功能性
- ☐ B、可用性
- ☐ C、保障性

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、符合性

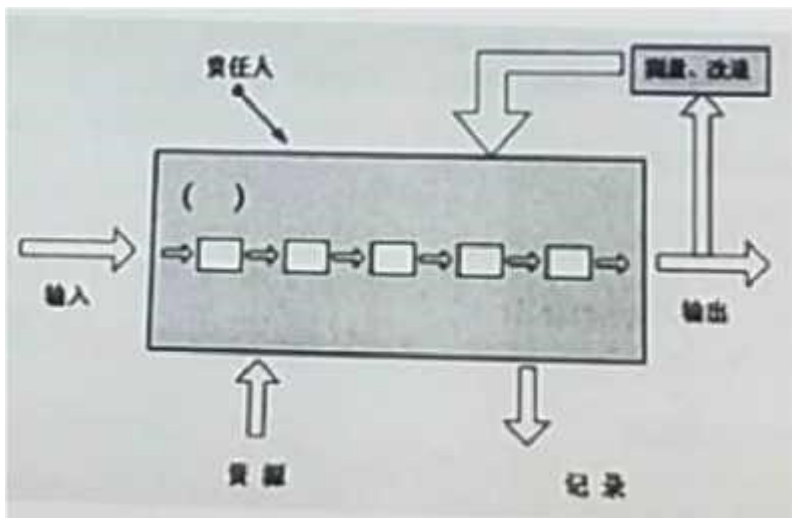
✔ 回答正确

+1分

68、SO9001 - 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对采用的过程方法，通过满足顾客要求，增进顾客满意，下图是关于过程方法示意图，空白

分值1分

处应填写 ( )



○ A、策略

○ B、管理者

○ C、组织

● D、活动

✔ 回答正确

+1分

69、作为信息安全从业人员，以下那种行为违反了CISP 职业道德准则 ( ) 分值1分

○ A. 抵制通过网络系统侵犯公众合法权益

● 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

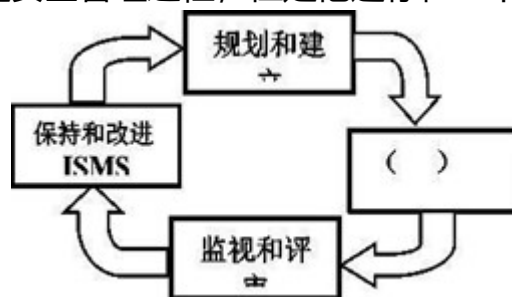
○ D. 帮助和指导信息安全同行提升信息安全保障知识和能力

✔ 回答正确

+1分

70、小李在学习信息安全管理体系统(Information Security Management System,ISMS)的有关知识后，按照自己的理解画了一张图来描述安全管理过程，但是他还存在一个

空白处未填写，请帮他选择一个最合适的选项 ( )



分值1分

○ A. A.监控和反馈ISMS

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.实施和运行ISMS
- ☐ C.执行和检查ISMS
- ☐ D.沟通和咨询ISMS

✔ 回答正确

+1分

71、规范的实施流程和文档管理，是信息安全风险评估性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

72、若一个组织声称自己的ISMS 符合ISO/IEC 27001 或GB/T22080 标准要求，其信息安全控制措施通常要在物理和环境安全方面实施规划控制，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，关键或敏感的信息以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，下列不包括哪一项

（） 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

✔ 回答正确

+1分

73、.IPV 4 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 头部的校验和字段来保证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. ITSec 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

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

74、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.主体可以接收客体的信息和数据，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.对目录的访问权限可分为读、写和拒绝访问

✔ 回答正确

+1分

75、强制访问控制系统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类型，如BLP、Clark-Willson 和ChineseWall 等。小李自学了BLP 模型，并对该模型的特点进行了总结，以下四种对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”

✔ 回答正确

+1分

76、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. 高虚警率，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

77、小王在学习定风险评估方法后，决定试着为单位机房计算火灾的风险大小假设单位机房的总值为400万人民币，暴露系数(Exposure factor,EF)是 25%，年度发生率annualized rate of Occurrence,ARO),为0.2,那么小王计算的年度预期损失Annualized Loss Expectancy, AE)应该是（） 分值1分

- ☐ A、100 万人民币
- ☐ B、400 万人民币
- ☒ C、20 万人民币
- ☐ D、180万人民币

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



回答正确

+1分

78、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。假设单位机房的总价格为200 万元人民币，暴露系数(FoposureFactor.EF)是25%,年度发生率annualized rate of Occurrence,ARO)为0.1,那么小王计算的年度预期损失Annualized Loss Expectancy,AE)应该是 ( )， 分值1分

- ☒ A. 5 万元人民币
- ☐ B. 50 万元人民币
- ☐ C. 2.5 万元人民币
- ☐ D. 25万元人民币



回答正确

+1分

79、GP/T18336《信息技术安全性评估准则》是测评标准中的重要标准，该标准定义了保护轮廓(protectionprofile,pp)和安全目标(security target,st)的评估准则。提出了评估保证级(evaluation assurance level, .eal),期评估保证级共分为()个递增的评估保证等级 ( ) 分值1分

- ☐ A. 4
- ☐ B. 5
- ☐ C. 6
- ☒ D. 7



回答正确

+1分

80、某集团公司更具业务需要，在各地分支机构部署前置机，为了保证安全，将集团总部要求前置机开放日志由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，从而导致部分敏感信息泄露，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，但不能响系统使用，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

81、关于我国加强信息安全保障工作的主要原则，以下说法错误的是： ( ) 分值1分

- ☐ A. 立足国情，以我为主，坚持技术与管理并重
- ☐ B. 正确处理安全和发展关系，以安全保发展，在发展中求安全
- ☐ C. 统筹规划，突出重点，强化基础工作
- ☒ D. 全面提高信息安全防护能力，保护公众利益，维护国家安全



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

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，正确的理解是：（） 分值1分

- ☐ A. 测量单位是基本实施(base practices,bp)
- ☐ B. 测量单位是通用实施(Generic practices GP)
- ☐ C. 测量单位是过程区域(Process Areas,PA)
- ☒ D. 测量单位是公开特征(common features,cf)

✔ 回答正确

+1分

83、信息安全管理体(SMS)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ISKS 符合 1S0/IBC27001 或CB/T22080 标准要求，则需实施准要求，则需实施以下ISMS 建设的各项工作，哪不属于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

84、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、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

85、目前，很多行业用户在进行信息安全产品选项时，均要求产品高通过安全测评。关于信息安全产品测评的意义，下列说法中不正确的是：（） 分值1分

- ☐ A. 有助于建立和实施信息安全产品的市场准入制度
- ☐ B. 对用户采购信息安全产品，设计、建设、使用和管理安全的信息系统提供科学公正的专业指导
- ☐ C. 对信息安全产品的研究、开发、生产以及信息安全服务的组织提供严格的规范引导和质量监督
- ☒ D. 打破市场垄断，为信息安全产业发展创造一个良好的竞争环境

✔ 回答正确

+1分

86、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 $R(A, T, V)=R(L(T, v), F(l, a, V_a))$ 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

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. L 表示威胁利用资产脆弱性导致安全事件的可能性
- ☐ C. P 表示安全事件发生后造成的损失
- ☒ D. Ia, Va 风别表示安全事件作用全部资产的价值与其对应资产的严重程度

✔ 回答正确

+1分

87、IP 地址用来标识不同的网络、子网以及网络中的主机。所谓IP 地址规划。是推根据IP 编址特点，为所设计的网络中的节点、网络设备分配合适的IP 地址。如某个小型网络拥有10个与互联网直接连接的IP 地址，但是该网络内有15 台个人计算机假如这些计算机不会同时开 机并连接互联网，那么可以将这10 个互联网地址集中起来使用，当任意一台个人计算机开机 并连接网络时，管理中心从这10 个地址中任意抽取个尚未分配的IP 地址分配给这台计算机。他关机时，管理中心将该地址收回，并重新设置为未分配。那么上述的IP 地址分配方式属于（）， 分值1分

- ☒ A. 动态分配地址
- ☐ B.静态分配地址
- ☐ C.NAT 池分配地址
- ☐ D.端口MT 分配地址

✔ 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

分值1分

来形象表达，如下图所示，请问图中空（）



- ☐ A. 执行(do)
- ☒ B. 检测(detection)
- ☐ C. 数据(data)
- ☐ D. 持续(duration)白处应填写是( )

✔ 回答正确

+1分

89、小陈某电器城购买了一台冰箱，并留下了个人姓名、电话和电子邮件地址等信息，第二天他收了一封邮件他中奖的邮件，查看该邮件后他按照提示操作缴纳中奖税款后并没有得到中奖金，再成才得知电器城共没有中奖的活动、在此案例中，下面描述量误的是（） 分值1分

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

加微信：vic\_tom，进cisp考证备考群，请务必备注：备考

- ☐ A. 小陈应当注意保护自己的隐私，没有必要告诉别人的信息不要登记和公和给别人
- ☐ B. 小陈钱被偷走了，这类网络犯罪哪案件也应该向公安局报案
- ☐ C. 邮件服务运营高商通过技术手段，可以在一定程度上阻止此类的钓鱼邮件和明哄骗邮件
- ☒ D. 小陈应当向电器城索，追回损失

✔ 回答正确

+1分

90、下列选项中，哪个不是我国信息安全保障工作的主要内容：（） 分值1分

- ☐ A. 加强信息安全标准化工作,积极采用“等同采用、修改采用.制定”等多种方式,尽快建立标准体系
- ☒ B. 建立国家信息安全研究中心，加快建立国家急需的信息安全技术体系，实现国家信息安全自主可控目标
- ☐ C. 建设和完善信息安全基础设施，提供国家信息安全保障能力支撑
- ☐ D. 加快信息安全学科建设和信息安全人才培养

✔ 回答正确

+1分

91、有关能力成熟度模型（），错误的理解是：（） 分值1分

- ☒ A. CMM 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产品”

✔ 回答正确

+1分

92、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意见》

✔ 回答正确

+1分

93、关于恶意代码的守护程度的功能，以下说法正确的是：（） 分值1分

- ☐ A. 隐藏恶意代码
- ☐ B. 加大监测力度
- ☐ 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

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

94、实体身份鉴别的方法多种多样，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。如图，小王在登录某移动支付平台时，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

分值1分

使用自己的账户进行支付、转账等（）



- ☐ 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

95、某单位门户网站发完成后，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

96、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
- ☒ C、纵深防御原则
- ☐ D、最少共享机制原则

✔ 回答正确

+1分

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《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

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、风险分析
- ☐ D、风险结果判定

✔ 回答正确

+1分

98、在实施信息安全风险评估时，需要对资产的价值进行识别、分类和赋值，关于资产价值的评估，以下选项中正确的是（） 分值1分

- ☐ A、资产的价值指采购费用
- ☐ B、资产的价值指维护费用
- ☒ C、资产的价值与其重要性密切相关
- ☐ D、资产的价值无法估计

✔ 回答正确

+1分

99、CC 标准是目前系统安全认证方面最权威的标准，以下哪一项没有体现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T 产品的开发、生产、测试和评估过程中

✔ 回答正确

+1分

100、ISO 27002(Information technology- Securtiy Techniques-Code of practice for informationmanagement)是重要的信息安全管理标准之一，下图是关于其演进变化示意图，途中括号空白处应填写？（） 分值1分

- ☐ A.B.7799.1.3
- ☒ B..ISO17799
- ☐ C.AS/NZS4630
- ☐ D.NST SP 800 - 17

✔ 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



加微信：vic\_tom，进cisp考证备考群，请务必备注：备考



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

137\*\*\*\*4355 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