注册信息安全专业人员考试补充复习题（112 题）

1、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助 SDE 足微软 SM 中提出的威胁建模方法，将威胁分为六类， Spoofing-是 SRD 中欺编类的威胁，以下威胁中哪个可以归入此类威胁？ (D)

A、网站竞争对手可能雇佣攻击者实施 ds 攻击，降低网站访问速度

B、网站使用 http 协议进行河览等操作，未对数据进行加密，可能导放用户传输信思露，例如购买的商品金额等

C、网站使用 ht 协议进行河览等操作，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其他方式获得用户密码，以该用户身份登录修改用户订单信息

2、在国家标准 GBT20274.1-2006《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？(B)

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

3、以下哪种风险被认为是合理的风险 (D)

A、最小的风险

B、残余风险

C、未识别的

D、可接受的风险

4、关于源代码审核，下列说法正确的是 (D)

A、源代码市核往往需要大量的时间采用人工市核费时费力，但可以通过多人并行市核来弥补这个缺点

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 使用代码核王共动化行代吗检和分析，能够大提高软件可性开节省件开发和测试的成本，已经取代了人工审核方式

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胞藏的识和块陷

5、关于《网络安全法》域外适用效力的理解，以下哪项是错的 (A)

A、当前对于域外的网攻击，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成胁我国可以组织技术力量进行监测、防御和处置

C、对于米自境外的网络攻击我国可以追究其法律责任

D、对于来自境外的违法信息我国可以加以阻断传播

6、信息安全保障技术框架（ I nformation Assurance Technical Framework，IATF），目的是为保障政府和工业的()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；()、技术和运行（亦称为操作 (A)

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

7、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 (B)

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

8、与 PDR 模型相比，P2DR 模型则更强调()，即强调系统安全的()，并且以安全检测、()和自适应填充安全间隙为循环来提高()。 (D)

A、漏洞监测；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

9、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 (C)

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害，所以可以先不做处理

C、对于重要的服务，应在检测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

10、若一个组织生成自己的 ISMS 符合 SO/=C27001 或 GBT22080 标准要求，其信息安全控制实施通畅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(D)。

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

11、随着即时通讯软件的普及使用，即时通讯软件也被恶意代码利用进行传播，以下哪项功能不是恶意代码利用即时通讯进行传播及执行的方式(D)

A、利用即时通讯软件的发送功能发送带恶意代码的可执行文件

B、利用即时通讯软件发送制定恶意网页的 URL

C、利用即时通软件发送指向恶意地址的程序

D、利用即时通讯发送携带恶意代码的 TXT 文档

12、 SABSA 模型包括()它是一个()，它在第一层从安全的角度定义了 0)。模型的每一层在抽象方面逐层减少，细节逐层增加，因此，它的层级都是建在其他层之上的，从策略逐渐到几乎和解决方案的()。其思路上创新提出了一个包括战略、概念、设计、实施、度量和审计层次的(B)

A、五层；业务需求；分层模型；实施实践；安全链条

B、六层；分层模型；业务需求；实施实践；安全链条；

C、五层：分层模型；业务需求，实施实践；安全链条；

D、六层；分层模型：实施实践；也无需求；安全链条

13、关于信息安全管理体系的作用，下面理解错误的是(B)

A、对内而言,由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

14、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(D)
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

15、某商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应预案,在向主管领导写报告时,他列举了编制信息安全应急响应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(C)
A、应急预案是明确关键业务系统信息安全应急响应只会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措施

16、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,老王要求信息安全员给出解决措施,信息安全员给出了四条措施建议,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)。(C)
A、采购防病毒网关并部署在企业互联网出口中,实现对所有浏览网页进行检测,组织网页中的病毒进入内网
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

17、信息系统安全保障是在信息系统的整个生命周期中,通过对信息系统的风险分析,制定并执行相应的安全保障策略,从技术、管理、工程和人员等方面提出安全保障要求,确保信息系统的保密性、完整性和可用性,降低安全风险到可接受的成都,从而保障系统实现组织机构的业务。信息系统保障工作如图所示,从该图不难得出,信息系统是()。信息系统安全风险的因素主要有( ) (D)
A、用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和;信息系统自身存在的漏洞
B、用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和;信息系统来自系统外部的威胁
C、用于采集、处理整个基础设施、组织结构、人员和组件的总和;信息系统自身存在的漏洞和来自系统外部的威胁
D、用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结构、人员和组件的总和;信息系统自身存在的漏洞和来自系统外部的威胁

18、国际标准化组织(International Organization for Standardization,ISO)对信息安

全的定义为(D)

A、保护信息和信息系统不被未经授权的访问、使用、泄露、修改和破坏,为信息和信息系统提供保密性完整性、可用性、可控性和不可否认性

B、信息安全,有时缩写为 Infosec,是防止未经授权的访问、使用、披露、中断、修改、检查、记录或破坏信息的做法。它是一个可以用于任何形式数据(例如电子、物理)的通用术语

C、在既定的密级条件下,网络与信息系统抵御意外事件或恶意行为的能力,这些事件和行为将威胁所存储或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和机密性

D、为数据处理系统建立和采取技术、管理的安全保护,保护计算机硬件、软件、数据不因偶然的或恶意的原因而受到破坏、更改、泄露

19、若一个组织声称自己的 ISMS 符合 ISO/EC27001 或 GBT22080 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 (D)

A、任用之前

B、任用中

C、任用终止或变化

D、任用后

20、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(D)

A、P 是 Plan,指分析问题,发现问题,确定方针,目标和活动计划

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,找出效果

D、A 是 Aim,指瞄准问题,抓住安全事件的核心,确定责任

21、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。 (D)

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

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

22、作为单位新上任的 CSO,你组织了一次本单位的安全评估工作以了解单位安全现状。在漏洞扫描报告中,你发现了某部署在内网且对内部服务的业务系统存在一个漏洞,对比上一年度的漏洞扫描报告,发现这个漏洞之前已经报告出来,经询问安全管理员得知,这个业务系统开发商已经倒闭,因此无法修复。对于这个问题,你应该如何处理 (C)

A、向公司管理层提出此问题,要求立即立项重新开发此业务系统,避免单位中存在这样的安全风险

B、既然此问题不是新发现的问题,之前已经存在,因此与自己无关,可以不予理会

C、让安全管理人员重新评估此漏洞存在的安全风险并给出进一步的防护措施后再考虑如何处理

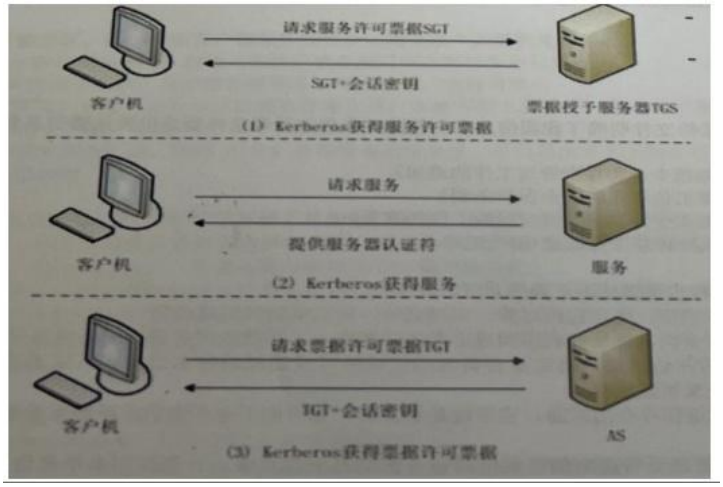
D、让安全管理员找出验收材料看看有没有该业务系统源代码,自己修改解决这个漏洞

23、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、威胁途径等多种因素,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 (C)

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

24、()第二十三条规定存储、处理国家秘密的就计算机信息系统(以下简称泄密信息系统)按照0实行分级保护。(0)应当按照国家保密标准配备保密设施、设备。①)、设备应当与涉密信息系统同步规划、同步建设、同步运行(三同步)。涉密信息系统应当按照规定,经0)后,方可投入使用 (A)
A、《保密法》:涉密程度;涉密信息系统;保密设施;检查合格
B、《国家保密法》涉密程度;涉密系统;保密设施;检查合格
C、《网络保密度;涉密系统;查合格
D、《安全保密度;涉密信息系施:检查合格

25、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(KDC)、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,分别为(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 (D)



A、1—2—3
B、3—2—1
C、2—1—3
D、3—1—2

26、企业安全架构(Sherwood Applied Business Security Architecture, SABSA)是企业架构的 个子集,它定义了0,包括各层级的()、流程和规程,以及它们与整个企业的战略、战术和运营链接的方式,用全面的、严格的方法描述了组成完整的信息安全管理体系(ISMS)所有组件的()。开发企业安全架构的很主要原因是确保安全工作以一个标准化的节省成本的方式与业务实践相结合。架构在抽象层面工作,它提供了一个0。除了安全性之外,这种类型的架构让组织更好的实现の、集成性、易用性、标准化和便于治理性。 (B)
A、信息安全战略;解决方案;结构和行为:可供参考的框架;互操作性
B、信息安全战略;结构和行为;解决方案;可供参考的框架;互操作性
C、信息安全战略;解决方案;可供参考的框架:;结构和行为;互操作性
D、信息安全战略;可供参考的框架;解决方案:结构和行为;互操作性

27、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病删除了系统中的数据,由于系统备份是每周六进行一次,时间发生时间为周三,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》,该事件的标准分类和定级应该是(D)

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)

28、在PDR模型的基础上发展成为(Policy- Protection- Detection- Response,PPDR)模型,即策略防护-检测响应。模型的核心是所有的防护、检测、响应都是依据安全策略实施的。在PPDR模型中,策略指的是信息系统的安全策略,包括访问控制策略、加密通信策略、身份认证策略、备份恢复策略等。策略体系的建立包括安全策略的制定、()等;防护指的是通过部署和采用安全技术来提高网络的防护能力如()、防火墙、入侵检测、加密技术、身份认证等技术检测指的是利用信息安全检测工具,监视、分析、审计网络活动了解判断网络系统的()。检测这一环节,使安全防护从被动防护演进到主动防御是整个模型动态性的体现。主要方法包括实时监控、检测、报警等响应指的是在检测到安全漏洞和安全事件时通过及时的响应措施将网络系统的()调整到风险最低的状态,包括恢复系统功能和数据,启动备份系统等。其主要方法包括关闭服务、跟踪、反击、消除影响等 (A)

A.评估与执行;访问控制;安全状态安全性

B.评估与执行;安全状态;访问控制;安全性

C.访问控制;评估与执行;安全状态;安全性

D.安全状态;评估与执行;访问控制;安全性

29、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[20091812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[20101003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(C)

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

D.测评体系;等级保护评估中心;能力验证;等级测评;取消授权

30、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0)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 (A)

A.GB/T22239-2008《信息系统安全等级保护基本要求》

B.GB/T2224の-208《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》

31、以下关于威胁建模流程步骤说法不正确的是(D)

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.消减威脉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

32、有关系统安全工程-能力成熟度模型(SSE-CMM)错误的理解是(C)

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

33、根据相关标准，信息安全风险管理可分为背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询等阶段，按照该框架，文档《风险分析报告》应该属于那个阶段的输出成果(A)

A. 风险评估
B. 风险处理
C. 批准监督
D. 监控审查

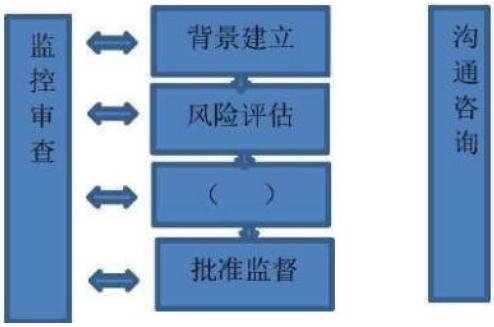
34、根据《关于开展信息安全风险评估工作的意见》的规定，错误的是(A)

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

35、即使最好用的安全产品也存在（），结果，在任何的系统中敌手最终都能够找到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。(B)

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

36、我国标准《信息安全风险管理指南》(GB/Z 24364)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 (D)

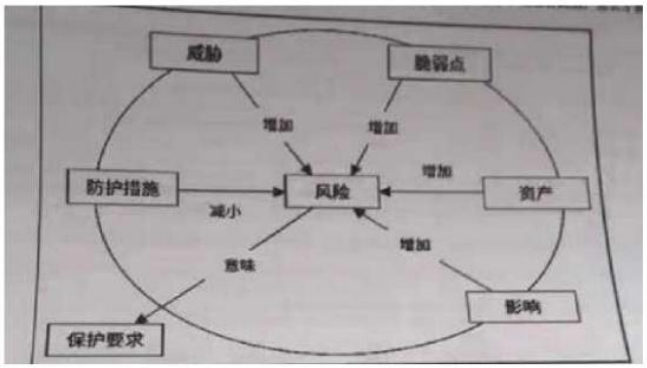


A. 风险计算
B. 风险评估
C. 风险预测
D. 风险处理

37、在国家标准，GBT202741-2006《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？(B)

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

38、风险,在 GBT22081 中定义为时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。 SO/EC13335-1 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?(A)



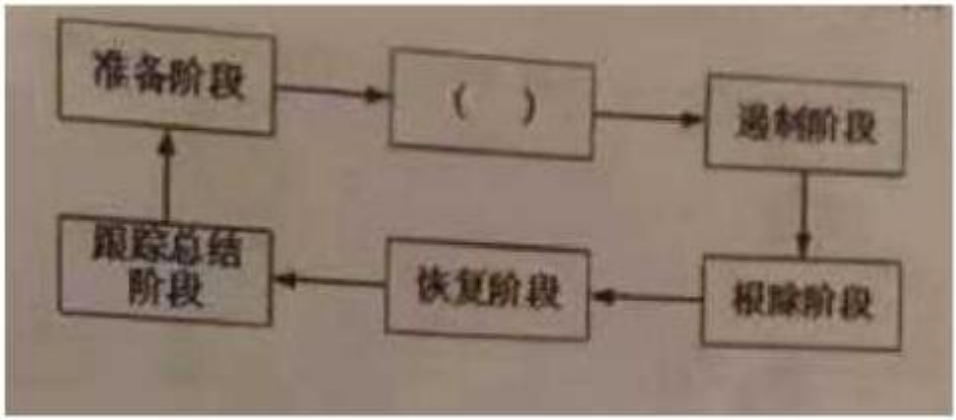
A、组织应该根据风险建立响应的保护要求,通过构架防护措施降低风险对组织产生的影响
B、加强防护措施,降低风险
C、减少威胁和脆弱点,降低风险
D、减少资产降低风险。

39、有关危害国家秘密安全的行为的法律责任,正确的是(A)
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,不需承担刑事责任;
D、承担了刑事责任,无需再承担行政责任和/或其他处分

40、分布式拒绝服务(Distributed Denial of Service,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。般来说,DDoS 攻击的主要目的是破坏目标系统的(C)
A、保密性
B、完整性
C、可用性
D、真实性

41、部署互联网协议安全虚拟专用网(nternet Protocol Security Virtual Private NetworkIpsec VPN)时,以下说法正确的是(C)
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 网络是,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

42、为了能够合理、有序地处理安全事件,应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。 PDCERF 方法论是一种广泛使用的方法,其将应急响应分为六个阶段,如下图所示,请为图中括号空白处选择合适的内容(D)



A、培训阶段
B、文档阶段
C、报告阶段
D、检测阶段

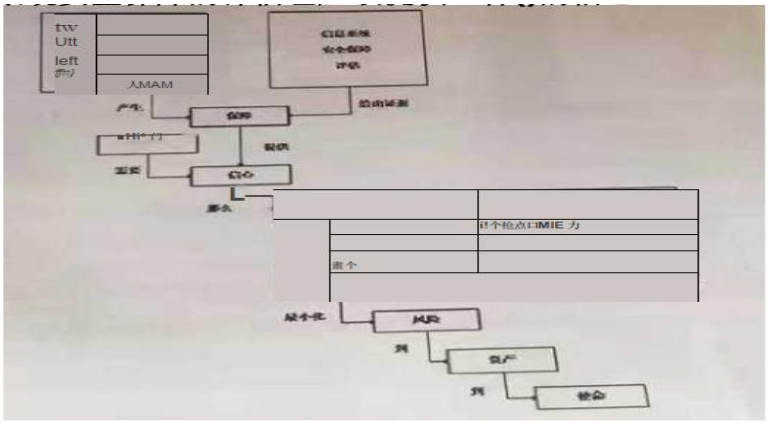
43、对于关键信息基础设施的外延范围，以下哪项是正确的(C)
A、关键信息基础设施的认定由国家网信部门确定，网络运营者自身及上级主管部门不能认定
B、关键信息基础设施与等级保护三级以上系统的范围一致，对于等级保护三级以上系统就应纳入关键信息基础设施保护范围
C、关键信息基础设施的具体范围由国务院制定，鼓励网络运营者自愿参照关键信息基础设施保护标准要求开展保护
D、关键信息基础设施只限于公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务这七个行业，除此以外行业的网络不能认定为关键信息基础设施

44、保护-监测-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0)，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。(C)
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
D、信息安全保障；威胁；信息系统；检测工作

45、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，他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，以下选项中优先级最低的是(D)
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全培训，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

46、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成都的主观信心。信息系统安全保障评估的评估对象是()，信息系统不仅包含了仅讨论技术的信息技术系统，还包括同信息系统所处的运行环境相关的人和管理等领域。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 0 的信心。 (B)



A、安全保障工作;客观证据;信息系统;生命周期:动态持续
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

47、《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，安标志着我国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而()的渗透了我国()的各项工作。 (D)

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

48、老王是某政府信息中心主任，以下哪项是符合《保守国家秘密法》要求的 (D)

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维修
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插座应该与涉密信息系统同步投入使用

49、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 (A)

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题内容可以按照技术，管理和工程等方面需求展开编写

50、一个密码系统至少由明文、密文、加密算法、解密算法和密钥 5 部分组成，根据科克霍夫原则，其安全性是由下列哪个选项决定的 (D)

A、加密算法
B、解密算法
C、加密和解密算法
D、密钥

51、由于信息系统的复杂性，因此需要一个通用的框架对其进行解构和描述，然后再基于此

框架讨论信息系统的()。在 LATF 中,将信息系统的信息安全保障技术层面分为以下四个焦点领域:():区域边界即本地计算环境的外缘;();支持性基础设施,在深度防御技术方案中推荐()原则、()原则。 (C)

A. 网络和基础设施;安全保护问题:本地的计算机环境;多点防御;分层防御
B. 安全保护问题:本地的计算机环境;多点防御;网络和基础设施;分层防御
C. 安全保护问题;本地的计算机环境;网络和基础设施;多点防御;分层防御
D. 本地的计算环境;安全保护问题;网络和基础设施;多点防御;分层防御

52、以下关于数字签名说法正确的是 (D)

A. 数字签名是在所传输的数据后附加上一段和传输数据毫无关系的数字信息
B. 数字签名能够解决数据的加密传输,即安全传输问题
C. 数字签名一般采用对称加密机制
D. 数字签名能够解决篡改、伪造等安全性问题

53、以下关于法律的说法错误的是(B)

A. 法律是国家意志的统一体现,有严密的逻辑体系和效力
B. 法律可以是公开的,也可以是“内部”的
C. 一旦制定,就比较稳定,长期有效,不允许经常更改
D. 法律对违法犯罪的后果由明确规定,是一种“硬约束”

54、PKI 的主要理论基础是(B)

A、对称密码算法
B、公钥密码算法
C、量子算法
D、摘要算法

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的攻击,以下做法无用的是(B)

A、不下载、不执行、不接收来历不明的软件和文件
B、修改用户名和口令
C、不随意打开来历不明的邮件,不浏览不健康不正规的网站
D、安装反病毒软件和防火墙,安装专门的木马防范软件

56、以下关于 Web 传输协议、服务端和客户端软件的安全问题说法不正确的是(C)

A、HTTP 协议主要存在明文传输数据、弱验证和缺乏状态跟踪等方面的安全问题
B、HTP 协议缺乏有效的安全机制,易导致拒绝服务、电子欺骗、嗅探等攻击
C、 Cookie 是为了*别用户身份,进行会话跟踪而存储在用户本地终端上的数据,用户可以随意查看存储在 Cookie 中的数据,但其中的内容不能被修改
D、**HTTP 协议存在的安全问题,使用 HTTPS 具有较高的安全性,可以通过证书来验证服务器的身份,并为浏览器和服务器之间的通信加密

57、若一个组织声称自己的 ISMS 符合 SO/EC27001 或 GBT22080 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(C)

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、通信安全、合规性

D.在安全区域工作,公共访问、交接区安全

58、2016年10月2ㄔ日,美国东部地区发生大规模断网事件,此次事件是由于美国主要DNS服务.DoS攻击所致,影响规模惊人,对人们成产生活造成严重影响,DDos攻击的主要目的是破坏系.(B)

A、保密性

B、可用性

C、不可否认性

D、抗抵赖性

59、以下有关系统工程说法错误的是(C)

A、系统工程不属于基本理论、也不属于技术基础,它研究的重点是方法论

B、系统工程的目的是实现总体效果最优化,即从复杂问题的总体入手,认为总体大于和,各部分虽然存在不足,但总体可以优化

C、系统工程只需使用定量分析的方法,通过建立实际对象的数学模型,应用合适的优化算法对模决…问题

D、霍尔三维结构将系统工程整个活动过程分为前后紧密衔接的7个阶段和7个步骤

60、以下关于 windows 操作系统身份标识与鉴别,说法不正确的是(B)

A、本地安全授权机构(SA)生成用户账户在该系统内唯一的安全标识符(SID

B、用户对鉴别信息的操作,如更改密码等都通过一个以 Administrator 权限运行的服务“ Security……”来实现

C、Windows 操作系统远程登录经历了 SMB 鉴别机制、LM 鉴别机制、NRLM 鉴别机制、Kerberos 鉴别体系等阶段

D、完整的安全标识符(SID)包括用户和组的安全描,48比特的身份特权、修订版本和可变的验证值

61、某T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CS,请你指出存在问题的是哪个总结?(D)

A、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。

B、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。

C、公司应急预案事件分类依据 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。预案符合国家相关标准。

D、公司成立了信息安全应急相应组织。该组织由业务和技术人员组成,划分成应急响应领导小组、技术保障小组、专家小组。实施小组和日常运行小组。

62、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(D)

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事件的应急响应工作主要包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

63、下列关于软件安全开发中的BSI(Build security In)系列模型说法错误的是(D)

A.BSL 含义是指将安全内建到软件开发过程中,而不是可有可无,更不是游离于软件开发生命周期之外

B.软件安全的三根支柱是风险管理、软件安全触点和安全知识

C.软件安全触点是软件开发生命周期中一套轻量级最优工程化方法,它提供了从不同角度保

障安全的行为方式
D.BSI 系列模型强调安全测试的重要性,要求安全测试贯穿整个开发过程及软件生命周期

64、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(C)
A.要求所有的开发人员参加软件安全开发知识培训
B.要求规范软件编码,并制定公司的安全编码准则
C.要求开发人员采用瀑布模型进行开发
D.要求邀请专业队伍进行第三方安全性测试,尽量从多角度发现软件安全问题

65、GB/T220802008《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模型进行,及信息安全管理体系应建立 ISMS,实施和运行 SMS,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 (D)
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

66、我国等级保护政策发展的正确顺序是 (C)
①等级保护相关政策文件颁布
②计算机系统安全保护等级划分思想提出
③等级保护相关标准发布
④网络安全法将等级保护制度作为基本策
⑤等级保护工作试点
A.①②③④⑤
B.②③①⑤④
C.②⑤①③④
D.①②④③⑤

67、以下哪一个是国际标准化组织? (C)
A. ITEF
B. ITU-T
C. ISO
D. NIST

68、 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( )。
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

69、 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( )
A、安全凭证 B、用户名 C、加密密钥 D、会话密钥
注解:安全凭证指的是服务许可票据。

70、 以下关于 Windows 操作系统身份标识与鉴别，说法不正确的是（）

A. 本地安全授权机构（LSA）生成用户账户在该系统内唯一的安全标识符（SID）

B. 用户对鉴别信息的操作，如更改密码等都通过一个以 Administrator 权限运行的服务“Security Accounts Manager”来实现

C. Windows 操作系统远程登录经历了 SMB 鉴别机制、LM 鉴别机制、Kerberos 鉴别体系等阶段

D. 完整的安全标识符（SID）包括用户和组的安全描述，48 比特的身份特权、修订版本和可变的验证值

71、 目前，信息系统面临外部攻击者的恶意攻击威胁，从威胁能力和掌握资源分，这些威胁可以按照 个人或胁、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（ ）

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

72、 以下关于互联网协议安全(Internet Protocol Security，IPSec)协议说法错误的是？

A. 在传送模式中，保护的是 IP 负载

B. 验证头协议(Authentication Header，AH)和 IP 封装安全载荷协议(Encapsulating 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 Internet Protocol ，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

73、 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:

A. 系统安全工程能力成熟度模型（SSE-CMM）定义了 6 个能力级别，当工程队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，每次执行结果质量必须相同。

C. 系统安全工程能力成熟度模型（SSE-CMM）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科学的区别和独立性。

74、 下列关于软件安全开发中的 BSI（Build Security In)系列模型说法错误的是（）

A、BIS 含义是指将安全内建到软件开发过程中，而不是可有可无，更不是游离于软件开发生命周期之外

B、软件安全的三根支柱是风险管理、软件安全触点和安全知识

C、软件安全触点是软件开发生命周期中一套轻量级最优工程化方法，它提供了从不同角度保障安全的行为

D、BSI 系列模型强调安全测试的重要性，要求安全测试贯穿整个开发过程及软件生命周期

75、 即使最好用的安全产品也存在（）。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。一种有效的对策时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。

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；保护和监测

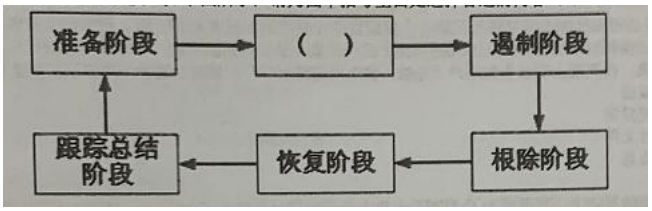
76、 保护-检测-响应（Protection-Detection-Response,PDR）模型是（）工作中常用

的模型，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。
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；检测工作
C. 信息安全保障；信息系统；威胁；检测工作
D. 信息安全保障；威胁；信息系统；检测工作

77、 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都门来测评和检查。此类信息系统应属于:
A. 零级系统 B.一级系统 C. 二级系统 D. 三级系统

78、 关于信息安全管理体系(Information Security Management Systems,ISMS)，下面描述错误的是( )。
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(Management Systems)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ISO27001 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

79、 为了能够合理、有序地处理安全事件，应事件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 方法论是一种防范使用的方法，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（ ）



A. 培训阶段 B.文档阶段 C. 报告阶段 D.检测阶段

80、 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（ ）
A. 准备阶段
B. 检测阶段
C. 遏制阶段
D. 根除阶段

81、 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（）
A、任用之前 B、任用中 C、任用终止或变化 D、任用后

82、 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（ ）

A. 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

B. 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

C. 信息中心的考虑是正确的，在软件开发需求分析阶段开始考虑安全问题，总体经费投入比软件运行后的费用要低

D. 软件开发部门的说法是正确的，因为软件出现安全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

83、 金女士经常通过计算机在互联网上购物，从安全角度看，下面哪项是不好的习惯？

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史记录和表单数据

84、 .关于《网络安全法》域外适用效力的理解，以下哪项是错误的（ ）

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

85、 国际标准化组织(Intermtional Organization for Standardization.ISO)对信息安全的定义为( )

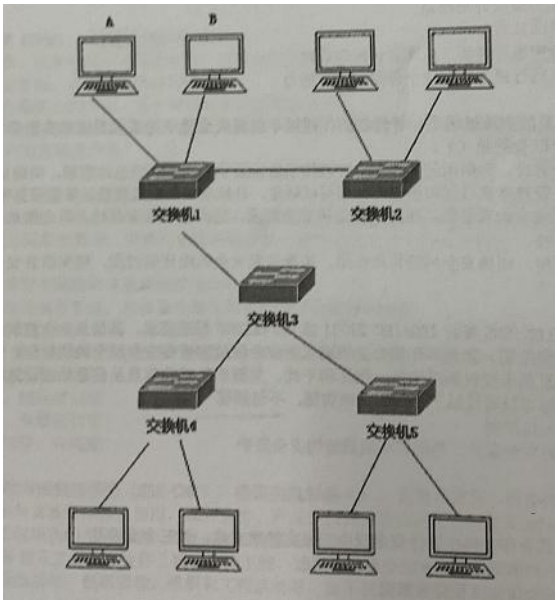
A. 保护信息和信息系续不被未经授权的访问、使用、泄露、修改和破坏，为信息和信息系统提供保密性、完整性 可用性、可控性和不可否认性

B. 信息安全，有时编写为 InfoSec，是防止未经授权的访网、使用、被露、中断、修改、检查、记录成破坏信息的做法。它是一个可以用于任何形式数据(例如电子、物理)的通用术语

C. 在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力，这些事件和行为将威胁所存储或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和机密性

D. 为数据处理系统建立和采取技术、管理的安全保护,保护计算机硬件、软件、数据不因 偶然的或恶意的原因而受到破坏、更改、泄露

86、 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其他所有端口,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 （ ）



A. 配置虚拟专用网络
B. 动态分配地址
C. 为路由交换设备修改默认口令
D. LAN 划分

87、 《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。
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. 总体要求；主要原则；总体纲领；展开；信息安全保障建设
D. 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

88、 关于 ARP 欺骗原理和防范措施，下面理解错误的是（ ）
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 APP 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 地址和其地主机进行连接

89、 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（ ）。
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

90、 在 PDR 模型的基础上，发展成为了(Policy-Protection-Detection-Response，PPDR)模型，既策略-防护-检测-响应。模型的核心是：所有的防护、检测、响应都是依据安全策

略实施的。在 PPDR 模型中，策略指的是信息系统的安全策略，包括访问控制策略、加密通信策略、身份认证策略、备份恢复策略等。策略体系的建立包括安全策略的制定、() 等；防护指的是通过部署和采用安全技术来提高网络的防护能力，如 ()、防火墙、入侵检测、加密技术、身份认证等技术；检测指的是利用信息安全检查工具，监视、分析、审计网络活动，了解判断网络系统的 ()。检测这一环节，使安全防护从被动防护演进到主动防御，是整个模型动态性的体现。主要方法包括：试试监控、检测、报警等；响应指的是在检测到安全漏洞和安全事件时，通过及时的响应措施将网络系统的 () 调整到风险最低的状态，包括回复系统功能和数据，启动备份系统等。其主要方法包括：关闭服务、跟踪、反击、消除影响等。

A. 评估与执行；访问控制；安全状态；安全性

B. 评估与执行；安全状态；访问控制；安全性

C. 访问控制；评估执行；安全状态；安全性

D. 安全状态；评估与执行；访问控制；安全性

91、 以下关于项目的含义，理解错误的是( )。

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(Agree to)、现实 (Realistic)、有一定的时限 (Time-oriented)

92、 PKI 的主要理论基础是 ( )。

A.对称密码算法 B.公钥密码算法 C.量子密码 D.摘要算法 答案:

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

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 端自行升级

94、 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的 FIP 服务存在高 风险漏洞。随后该单位在风险处理时选择了安装 FTP 服务洞补丁程序并加固 FTP 服务安 全措施，请问该措施属于哪种风险处理方式

A.风险降低 B. 风险规避 C.风险转移 D.风险接受

95、 以下关于 Web 传输协议、服务端和客户端软件的安全问题说法不正确的是( )。

A. HTTP 协议主要存在明文传输数据、弱验证和缺乏状态跟踪等方面的安全问题

B. HTTP 协议缺乏有效的安全机制，易导致拒绝服务、电子欺骗、嗅探等攻击

C. Cookie 是为了辨别用户身份，进行会话跟踪而存储在用户本地终端上的数据，用户可以随意查看存储在 Cookie 中的数据，但其中的内容不能被修改

D. 针对 HTP 协议存在的安全问题，使用 HTTPS 具有较高的安全性，可以通过证书来验证服务器的身份，并为浏览器和服务器之间的通信加密

96、 随着计算机在商业和民用领域的应用，安全需求变得越来越多样化，自主访问控制和强制访问控制难 以适应需求，基于角色的访问控制（RBAC）逐渐成为安全领域的一个研

究热点。RBAC 模型可以分为 RBAC0、RBAC1、RBAC2 和 RBAC3 四种类型，它们之间存在相互包含关系。下列选项中，对它们关系描述错 误的是（ ）。
A. RBAC0 是基于模型，RBAC1、RBAC2 和 RBAC3 都包含 RBAC0
B. RBAC1 在 RBAC0 的基础上，加入了角色等级的概念
C. RBAC2 在 RBAC1 的基础上，加入了约束的概念
D. RBAC3 结合 RBAC1 和 RBAC2，同时具备角色等级和约束

97、 关于标准，下面哪项理解是错误的（ ）
A. 标准是在一定范围内为了获得最佳秩序，经协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，标准是标准化活动的重要成果
B. 国际标准是由国际标准化组织通过并公布的标准，同样是强制性标准，当国家标准和国际标准的条款
C. 行业标准是针对没有国家标准而又才需要在全国某个行业范围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度，并报国务院标准化行政主管部门和国务院 有关行政主管培训部门备案，在公布国家标准后，该地方标准即应废止。

98、 2016 年 10 月 21 日，美国东部地区发生大规模断网事件，此次事件是由于美国主要 DNS 服务商 Dyn 遭遇大规模 DDos 攻击所致，影响规模惊人，对人们生产生活造成严重影响。 DDoS 攻击的主要目的是破坏系统的（ ）
A.保密性 B.可用性 C.不可否认性 D. 抗抵赖性

99、 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（ ）。
A. 要求所有的开发人员参加软件安全意识培训
B. 要求规范软件编码，并制定公司的安全编码准则
C. 要求增加软件安全测试环节，尽早发现软件安全问题
D. 要求开发人员采用瀑布模型进行开发

100、 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 重要程度对信息进行划分，不属于正确划分级别的是：
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

101、 随机进程名称是恶意代码迷惑管琊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（ ）。
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过程名称不固定，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

102、 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？

1. 模拟正常用户输入行为，生成大量数据包作为测试用例
2. 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
A. 监测和记录输入数据后程序正常运行的情况
B. 深入分析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

103、 CC 标准是目前系统安全认证方面最权威的而标准，那一项不是体现 CC 标准的先进性？
A. 结构开放性，即功能和保证要求可以“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

104、 以下关于网络安全设备说法正确的是（ ）。
A. 防火墙既能实现内外网物理隔离，又能实现内外网逻辑隔离
B. 安全隔离与信息交换系统也称为网闸,需要信息交换时,同一时间可以和两个不同安全级别的网络连接
C. 入侵检测系统的主要作用是发现并报告系统中未授权或违反安全策略的行为
D. .虚拟专用网是在公共网络中。利用隧道技术，建立一个永久、安全的通信网络

105、 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
B. 修改用户名和口令
C. 不随意打开来历不明的邮件，不浏览不健康不正规的网站
D. 安装反病毒软件和防火墙，安装专门的木马防治软件

106、 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：
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. 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

107、 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，有助于一个组织在事件发生时院止混乱的发生成是 在混配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，一种被广为按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> 送制>根除>>快复>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
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想响应规划过程中最关健的步理
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

108、 恢复时间目标(Recovery Time Objective，RTO)和恢复点目标(Recovery Point Objective，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(　)。

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

109、 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：

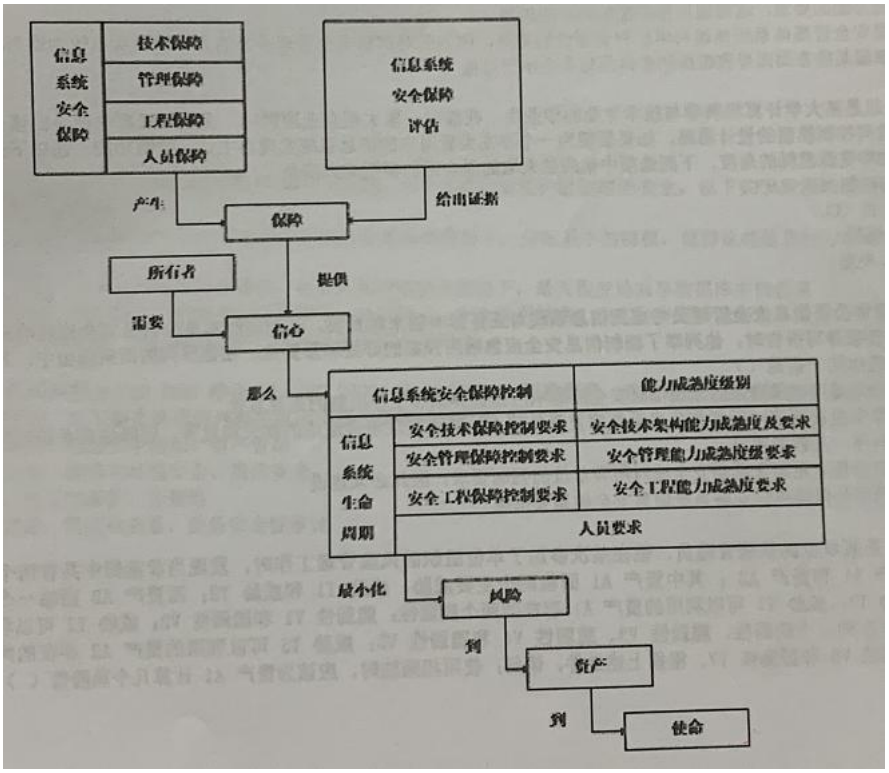
A. 最小特权原则

B. 职责分离原则

C. 纵深防御原则

D. 最少共享机制原则

110、 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()，信息系统不仅包含了仅讨论技术的信息技术系统，还包括同信息系统 所处的运行环境相关的人和管理等领域，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。



111、 安全保障工作:客观证据:信息系统;生命周期;动态持续

A. 客观证据:安全保障工作;信息系统:生命周期:动态持续

B. 客观证据：安全保障工作；生命周期：信息系统：动态持续

C. 客观证据：安全保障工作；动态持续；信息系统：生命周期

112、　私有 IP 地址是一段保留的 IP 地址。只适用在局域网中，无法在 Internet 上使用。私有地址，下面描述正 确的是？

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