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

A．这些行业都关系到国计民生，对经济运行和国家安全影响深远

B．这些行业都是信息化应用广泛的领域

C.这些行业信息系统普遍存在安全隐患，而且信息安全专业人才缺乏的现象比其他行业更突出

D．这些行业发生信息安全事件，会造成广泛而严重的损失

C

2．关于我国信息安全保障工作发展的几个阶段，下列哪个说法不正确：

A．2001-2002 年是启动阶段，标志性事件是成立了网络与信息安全协调小组，该机构是我国信息安全保障工作的最高领导机构 信息化领导小组（27 号文） 网络安全委员会

B．2003-2005 年是逐步展开和积极推进阶段，标志性事件是发布了指导性文件《关于加强信息安全保障工作的意见》(中办发 27 号文件)并颁布了国家信息安全战略

C．2005-至今是深化落实阶段，标志性事件是奥运会和世博会信息安全保障取得圆满成功

D．2005-至今是深化落实阶段，信息安全保障体系建设取得实质性进展，各项信息安全保障工作迈出了坚实步伐

A

3．依据国家标准/T20274《信息系统安全保障评估框架》，信息系统安全目标(ISST)中，安全保障目的指的是：

A、信息系统安全保障目的

B、环境安全保障目的

C、信息系统安全保障目的和环境安全保障目的

D.信息系统整体安全保障目的、管理安全保障目的、技术安全保障目的和工程安全保障目的

D

4．以下哪一项是数据完整性得到保护的例子?

A．某网站在访问量突然增加时对用户连接数量进行了限制，保证已登录的用户可以完成操作

B．在提款过程中 ATM 终端发生故障，银行业务系统及时对该用户的账户余额进行了冲正操作

C．某网管系统具有严格的审计功能，可以确定哪个管理员在何时对核心交换机进行了什么操作

D．李先生在每天下班前将重要文件锁在档案室的保密柜中，使伪装成清洁工的商业间谍无法查看

B

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

A.乙对信息安全不重视，低估了黑客能力，不舍得花钱

B．甲在需求分析阶段没有进行风险评估，所部署的加密针对性不足，造成浪费

C．甲未充分考虑网游网站的业务与政府网站业务的区别

D．乙要综合考虑业务、合规性和风险，与甲共同确定网站安全需求

A

6．进入 21 世纪以来，信息安全成为世界各国安全战略关注的重点，纷纷制定并颁布网络空间安全战略，但各国历史、国情和文化不同，网络空间安全战略的内容也各不相同，以下说法不正确的是：

A．与国家安全、社会稳定和民生密切相关的关键基础设施是各国安全保障的重点

B．美国尚未设立中央政府级的专门机构处理网络信息安全问题，信息安全管理职能由不同政府部门的多个机构共同承担

C．各国普遍重视信息安全事件的应急响应和处理 p24

D．在网络安全战略中，各国均强调加强政府管理力度，充分利用社会资源，发挥政府与企业之间的合作关系

B

7．与 PDR 模型相比，P2DR 模型多了哪一个环节?

A．防护

B．检测

C．反应

D.策略

D

8．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)

B

9.2008 年 1 月 2 日,美目发布第 54 号总统令,建立国家网络安全综合计划(Comprehensive National Cybersecurity Initiative，CNCI)。CNCI 计划建立三道防线：第一道防线，减少漏洞和隐患，预防入侵；第二道防线，全面应对各类威胁；第三道防线，强化未来安全环境．从以上内容，我们可以看出以下哪种分析是正确的：

A．CNCI 是以风险为核心，三道防线首要的任务是降低其网络所面临的风险

B.从 CNCI 可以看出，威胁主要是来自外部的，而漏洞和隐患主要是存在于内部的

C．CNCI 的目的是尽快研发并部署新技术彻底改变其糟糕的网络安全现状，而不是在现在的网络基础上修修补补

D．CNCI 彻底改变了以往的美国信息安全战略，不再把关键基础设施视为信息安全保障重点，而是追求所有网络和系统的全面安全保障

A

10．下列对于信息安全保障深度防御模型的说法错误的是：

A．信息安全外部环境：信息安全保障是组织机构安全、国家安全的一个重要组成部分，因此对信息安全的讨论必须放在国家政策、法律法规和标准的外部环境制约下。

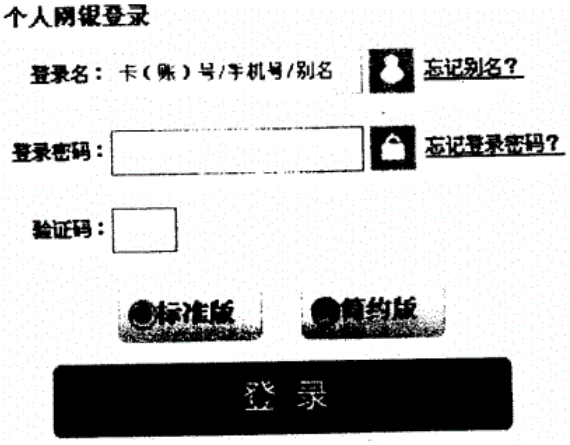
B．信息安全管理和工程：信息安全保障需要在整个组织机构内建立和完善信息安全管理体系，将信息安全管理综合至信息系统的整个生命周期，在这个过程中，我们需要采用信息系统工程的方法来建设信息系统。

C．信息安全人才体系：在组织机构中应建立完善的安全意识，培训体系也是信息安全保障的重要组成部分。

D．信息安全技术方案：“从外而内、自下而上、形成边界到端的防护能力”。

D

11．如图，某用户通过账号、密码和验证码成功登录某银行的个人网银系统，此过程属于以下哪一类：



A．个人网银系统和用户之间的双向鉴别

B．由可信第三方完成的用户身份鉴别

C.个人网银系统对用户身份的单向鉴别

D．用户对个人网银系统合法性的单向鉴别

C

12．如下图所示，Alice 用 Bob 的密钥加密明文，将密文发送给 Bob。Bob 再用自己的私钥解密，恢复出明文。以下说法正确的是：

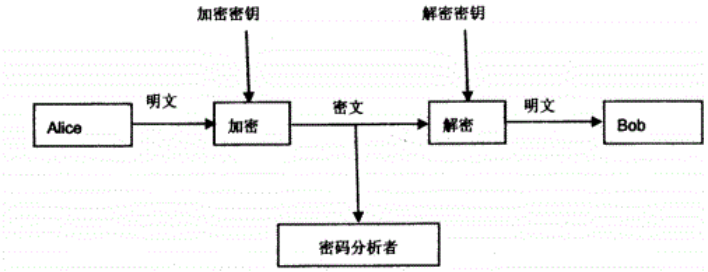
A．此密码体制为对称密码体制

B．此密码体制为私钥密码体制

C．此密码体制为单钥密码体制

D．此密码体制为公钥密码体制

D



13．下列哪一种方法属于基于实体“所有”鉴别方法：

A．用户通过自己设置的口令登录系统，完成身份鉴别

B．用户使用个人指纹，通过指纹识别系统的身份鉴别

C．用户利用和系统协商的秘密函数，对系统发送的挑战进行正确应答，通过身份鉴别

D.用户使用集成电路卡(如智能卡)完成身份鉴别

D

14．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?

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

A

15．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性测试，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?

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期产生的漏洞

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

A

16．软件安全设计和开发中应考虑用户稳私包，以下关于用户隐私保护的说法哪个是错误的?

A．告诉用户需要收集什么数据及搜集到的数据会如何披使用

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稳私数据，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

C

17．软件安全保障的思想是在软件的全生命周期中贯彻风险管理的思想，在有限资源前提下实现软件安全最优防护，避免防范不足带来的直接损失，也需要关注过度防范造成的间接损失。在以下软件安全开发策略中，不符合软件安全保障思想的是：

A.在软件立项时考虑到软件安全相关费用，经费中预留了安全测试、安全评审相关费用，确保安全经费得到落实

B．在软件安全设计时，邀请软件安全开发专家对软件架构设计进行评审，及时发现架构设计中存在的安全不足

C．确保对软编码人员进行安全培训，使开发人员了解安全编码基本原则和方法，确保开发人员编写出安全的代码

D．在软件上线前对软件进行全面安全性测试，包括源代码分析、模糊测试、渗透测试，未经以上测试的软件不允许上线运行

D

18．以下哪一项不是工作在网络第二层的隧道协议：

A.VTP

B．L2F

C．PPTP

D．L2TP

A

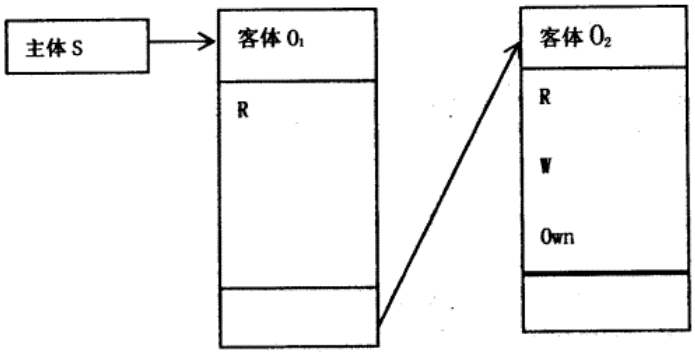
19．如圈所示，主体 S 对客体 01 有读(R)权限，对客体 02 有读(R)、写(W)、拥有(Own)权限，该图所示的访问控制实现方法是：

A．访问控制表(ACL)

B．访问控制矩阵

C.能力表(CL)

D. 前缀表(Profiles)



C

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

A. 当用户请求访问某资源时，如果其操作权限不在用户当前被激活角色的授权范围内，访问请求将被拒绝

B. 业务系统中的岗位、职位或者分工，可对应 RBAC 模型中的角色

C. 通过角色，可实现对信息资源访问的控制

D.RBAC 模型不能实现多级安全中的访问控制

D

21. 下面哪一项不是虚拟专用网络(VPN)协议标准：

A. 第二层隧道协议(L2TP)

B. Internet 安全性(IPSEC)

C.终端访问控制器访问控制系统(TACACS+)

D. 点对点隧道协议(PPTP)

C

22. 下列对网络认证协议(Kerberos)描述正确的是：

A. 该协议使用非对称密钥加密机制

B. 密钥分发中心由认证服务器、票据授权服务器和客户机三个部分组成

C．该协议完成身份鉴别后将获取用户票据许可票据

D．使用该协议不需要时钟基本同步的环境

C

23．鉴别的基本途径有三种：所知、所有和个人特征，以下哪一项不是基于你所知道的：

A．口令

B．令牌

C．知识

D．密码

B

24．在ISO的OSI安全体系结构中，以下哪一个安全机制可以提供抗抵赖安全服务？

A．加密

B.数字签名

C．访问控制

D．路由控制

B

25．某公司已有漏洞扫描和入侵检测系统(Intrusien Detection System，IDS)产品，需要购买防火墙，以下做法应当优先考虑的是：

A．选购当前技术最先进的防火墙即可

B．选购任意一款品牌防火墙

C．任意选购一款价格合适的防火墙产品

D．选购一款同已有安全产品联动的防火墙

D

26．在OSI参考模型中有7个层次，提供了相应的安全服务来加强信息系统的安全性，以下哪一层提供了保密性、身份鉴别、数据完整性服务？

A.网络层

B．表示层

C．会话层

D．物理层

B

27．某单位人员管理系统在人员离职时进行账号删除，需要离职员工所在部门主管经理

和人事部门人员同时进行确认才能在系统上执行，该设计是遵循了软件安全设计中的哪项原则?

A.最小权限

B.权限分离

C．不信任

D．纵深防御

B

28．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 Head，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

D

29．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，将威胁分为六类，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?

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信息

D

30.以下关于PGP(Pretty Good Privacy)软件叙述错误的是：

A．PGP可以实现对邮件的加密、签名和认证

B．PGP可以实现数据压缩

C．PGP可以对邮件进行分段和重组

D．PGP采用SHA算法加密邮件

PGP(Pretty Good Privacy)，是一个基于 RSA 公钥加密体系的邮件加密软件

D

31．入侵防御系统(IPS)是继入侵检测系统(IDS)后发展期出来的一项新的安全技术，它与 IDS 有着许多不同点，请指出下列哪一项描述不符合 IPS 的特点?

A．串接到网络线路中

B．对异常的进出流量可以直接进行阻断

C．有可能造成单点故障

D.不会影响网络性能

D

32．相比文件配置表(FAT)文件系统，以下哪个不是新技术文件系统(NTFS)所具有的优势?

A．NTFS 使用事务日志自动记录所有文件夹和文件更新，当出现系统损坏和电源故障等闯题而引起操作失败后，系统能利用日志文件重做或恢复未成功的操作

B．NTFS 的分区上，可以为每个文件或文件夹设置单独的许可权限

C．对于大磁盘，NTFS 文件系统比 FAT 有更高的磁盘利用率

D.相比 FAT 文件系统，NTFS 文件系统能有效的兼容 linux 下 EXT2 文件格式

D

33．某公司系统管理员最近正在部署一台 Web 服务器，使用的操作系统是 windows，在进行日志安全管理设置时，系统管理员拟定四条日志安全策略给领导进行参考，其中能有效应对攻击者获得系统权限后对日志进行修改的策略是：

A.在网络中单独部署 syslog 服务器,将 Web 服务器的日志自动发送并存储到该 syslog 日志服务器中

B.严格设置 Web 日志权限，只有系统权限才能进行读和写等操作

C．对日志属性进行调整，加大日志文件大小、延长日志覆盖时间、设置记录更多信息等

D．使用独立的分区用于存储日志，并且保留足够大的日志空间

A

34．关于 linux 下的用户和组，以下描述不正确的是__。

A．在 linux 中，每一个文件和程序都归属于一个特定的“用户”

B．系统中的每一个用户都必须至少属于一个用户组

C.用户和组的关系可以是多对一，一个组可以有多个用户，一个用户不能属于多个组

D．root 是系统的超级用户，无论是否文件和程序的所有者都具有访问权限

C

35．安全的运行环境是软件安全的基础，操作系统安全配置是确保运行环境安全必不可少的工作，某管理员对即将上线的 Windows 操作系统进行了以下四项安全部署工作，其中哪项设置不利于提高运行环境安全?

A．操作系统安装完成后安装最新的安全补丁，确保操作系统不存在可被利用的安全漏洞

B.为了方便进行数据备份，安装 Windows 操作系统时只使用一个分区 C，所有数据和操作系统都存放在 C 盘

C．操作系统上部署防病毒软件，以对抗病毒的威胁

D．将默认的管理员账号 Administrator 改名，降低口令暴力破解攻击的发生可能

B

36．在数据库安全性控制中，授权的数据对象_，授权子系统就越灵活?

A.粒度越小

B．约束越细致

C．范围越大

D．约束范围大

A

37．下列哪一些对信息安全漏洞的描述是错误的?

A．漏洞是存在于信息系统的某种缺陷。

B．漏洞存在于一定的环境中，寄生在一定的客体上(如 TOE 中、过程中等)。

C．具有可利用性和违规性，它本身的存在虽不会造成破坏，但是可以被攻击者利用，从而给信息系统安全带来威胁和损失。

D．漏洞都是人为故意引入的一种信息系统的弱点

D

38．账号锁定策略中对超过一定次数的错误登录账号进行锁定是为了对抗以下哪种攻击?

A．分布式拒绝服务攻击(DDoS)

B．病毒传染

C.口令暴力破解

D．缓冲区溢出攻击

C

39．数据在进行传输前，需要由协议栈自上而下对数据进行封装，TCP／IP 协议中，数据

封装的顺序是：

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

B

40．以下哪个不是导致地址解析协议(ARP)欺骗的根源之一？

A．ARP 协议是一个无状态的协议

B．为提高效率，ARP 信息在系统中会缓存

C．ARP 缓存是动态的，可被改写

D.ARP 协议是用于寻址的一个重要协议

D

41．张三将微信个人头像换成微信群中某好友头像，并将昵称改为该好友的昵称，然后向该好友的其他好友发送一些欺骗消息。该攻击行为属于以下哪类攻击？

A．口令攻击

B．暴力破解

C．拒绝服务攻击

D.社会工程学攻击

D

42．关于软件安全开发生命周期(SDL)，下面说法错误的是：

A．在软件开发的各个周期都要考虑安全因素

B．软件安全开发生命周期要综合采用技术、管理和工程等手段

C．测试阶段是发现并改正软件安全漏洞的最佳环节，过早或过晚检测修改漏洞都将增大软件开发成本

D．在设计阶段就尽可能发现并改正安全隐患，将极大减少整个软件开发成本

C

43．在软件保障成熟度模型(Software Assurance Maturity ldode，SAMM)中，规定了软件开发过程中的核心业务功能，下列哪个选项不属于核心业务功能：

A．治理，主要是管理软件开发的过程和活动

B.构造，主要是在开发项目中确定目标并开发软件的过程与活动

C．验证，主要是测试和验证软件的过程与活动

D.购置，主要是购买第三方商业软件或者采用开源组件的相关管理过程与活动

D

44．从系统工程的角度来处理信息安全问题，以下说法错误的是：

A．系统安全工程旨在了解企业存在的安全风险，建立一组平衡的安全需求，融合各种工程学科的努力将此安全需求转换为贯穿系统整个生存期的工程实施指南。

B．系统安全工程需对安全机制的正确性和有效性做出诠释，证明安全系统的信任度能够达到企业的要求，或系统遗留的安全薄弱性在可容许范围之内。

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

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

C

45．小王是某大学计算科学与技术专业的毕业生，大四上学期开始找工作，期望谋求一份技术管理的职位，一次面试中，某公司的技术经理让小王谈一谈信息安全风险管理中的“背景建立”的基本概念与认识，小王的主要观点包括：(1)背景建立的目的是为了明确信息安全风险管理的范围和对象，以及对象的特性和安全要求，完成信息安全风验管理项目的规划和准备；(2)背景建立根据组织机构相关的行业经验执行，雄厚的经验有助于达到事半功倍的效果；　(3)背景建立包括：风险管理准备、信息系统调查、信息系统分析和信息安全分析；(4)背景建立的阶段性成果包括：风险管理计划书、信息系统的描述报告、信息系统的分析报告、信息系统的安全要求报告。请问小王的所述论点中错误的是哪项：

A．第一个观点，背景建立的目的只是为了明确信息安全风险管理的范围和对象

B．第二个观点，背景建立的依据是国家、地区域行业的相关政策、法律、法规和标准

C.第三个观点，背景建立中的信息系统调查与信息系统分析是同一件事的两个不同名字

D．第四个观点，背景建立的阶段性成果中不包括有风险管理计划书

B

P66 页,此题目问的是小王的观点那条是错误的。第二个观点错误。选项中 C 选项是错误的，但是不是题目所问。

46．有关系统安全工程-能力成熟度模型(SSE-CMM)中的基本实施(Base Practices，BP)，

正确的理解是：

A．BP 是基于最新技术而制定的安全参数基本配置

B．大部分 BP 是没有经过测试的

C.一项 BP 适用于组织的生存周期而非仅适用于工程的某一特定阶段

D．一项 BP 可以和其他 BP 有重叠

C

47．以下哪一种判断信息系统是否安全的方式是最合理的?

A．是否已经通过部署安全控制措施消灭了风险

B．是否可以抵抗大部分风险

C．是否建立了具有自适应能力的信息安全模型

D.是否已经将风险控制在可接受的范围内

D

48．以下关于信息安全法治建设的意义，说法错误的是：

A．信息安全法律环境是信息安全保障体系中的必要环节

B．明确违反信息安全的行为，并对该行为进行相应的处罚，以打击信息安全犯罪活动

C．信息安全主要是技术问题，技术漏洞是信息犯罪的根源

D．信息安全产业的逐渐形成，需要成熟的技术标准和完善的技术体系

C

49．小张是信息安全风险管理方面的专家，被某单位邀请过去对其核心机房经受某种灾害的风险进行评估，已知：核心机房的总价价值一百万，灾害将导致资产总价值损失二成四(24%)，历史数据统计告知该灾害发生的可能性为八年发生三次，请问小张最后得到的年度预期损失为多少：

A．24 万

B．0．09 万

C．37．5 万

D.9 万

D

50．2005 年 4 月 1 日正式施行的《电子签名法》，被称为“中国首部真正意义上的信息化法律”，自此电子签名与传统手写签名和盖章具有同等的法律效力。以下关于电子签名说法错误的是：

A.电子签名——是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据

B．电子签名适用于民事活动中的合同或者其他文件、单证等文书

C．电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务

D．电子签名制作数据用于电子签名时，属于电子签名人和电子认证服务提供者共有

D 专有

51．风险管理的监控与审查不包含：

A．过程质量管理

B．成本效益管理

C．跟踪系统自身或所处环境的变化

D．协调内外部组织机构风险管理活动

D

52．信息安全等级保护分级要求，第三级适用正确的是：

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

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

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

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

B

53．下面哪一项安全控制措施不是用来检测未经授权的信息处理活动的：

A．设置网络连接时限

B．记录并分析系统错误日志

C．记录并分析用户和管理员操作日志

D．启用时钟同步

A

54．有关危害国家秘密安全的行为的法律责任，正确的是：

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

A

55．以下对于信息安全事件理解错误的是：

A．信息安全事件，是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件

B．对信息安全事件进行有效管理和响应，最小化事件所造成的损失和负面影响，是组织信息安全战略的一部分

C．应急响应是信息安全事件管理的重要内容

D.通过部署信息安全策略并配合部署防护措施，能够对信息及信息系统提供保护，杜绝信息安全事件的发生

D

56．假设一个系统已经包含了充分的预防控制措施，那么安装监测控制设备：

A．是多余的，因为它们完成了同样的功能，但要求更多的开销

B．是必须的，可以为预防控制的功效提供检测

C．是可选的，可以实现深度防御

D．在一个人工系统中是需要的，但在一个计算机系统中则是不需要的，因为预防控制的功能已经足够

B

57．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：

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的关系，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　不是原则，目的

D

58．以下哪一项不是信息安全管理工作必须遵循的原则?

A．风险管理在系统开发之初就应该予以充分考虑，并要贯穿于整个系统开发过程之中

B．风险管理活动应成为系统开发、运行、维护、直至废弃的整个生命周期内的持续性工

作

C．由于在系统投入使用后部署和应用风险控制措施针对性会更强，实施成本会相对较低

D．在系统正式运行后，应注重残余风险的管理，以提高快速反应能力

C

59.《信息安全技术　信息安全风险评估规范 GB／T 20984-2007》中关于信息系统生命周期各阶段的风险评估描述不正确的是：

A.规划阶段风险评估的目的是识别系统的业务战略，以支撑系统安全需求及安全战略等

B.设计阶段的风险评估需要根据规划阶段所明确的系统运行环境、资产重要性，提出安全功能需求

C.实施阶段风险评估的目的是根据系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全功能进行验证

D.运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种全面的风险评估。评估内容包括对真实运行的信息系统、资产、脆弱性等各方面

标准原文“较全面”

d

60．对信息安全风险评估要素理解正确的是：

A.资产识别的粒度随着评估范围、评估目的的不同而不同，既可以是硬件设备，也可以是业务系统，也可以是组织机构

B．应针对构成信息系统的每个资产做风险评价

C．脆弱性识别是将信息系统安全现状与国家或行业的安全要求做符合性比对而找出的差距项

D．信息系统面临的安全威胁仅包括人为故意威胁、人为非故意威胁

A

61．以下哪些是需要在信息安全策略中进行描述的：

A．组织信息系统安全架构

B.信息安全工作的基本原则

C、组织信息安全技术参数

D、组织信息安全实施手段

B

62．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.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

A

63．RPC 系列标准是由( )发布的：

A．国际标准化组织(ISO)

B．国际电工委员会(IEC)

C．国际贸易中心(ITC)

D.互联网工程任务组 IETF

D

64．对于数字证书而言，一般采用的是哪个标准?

A．ISO／IEC 15408

B．802．11

C．GB／T 20984

D．X.509

D

65．下面的角色对应的信息安全职责不合理的是：

A．高级管理层——最终责任

B.信息安全部门主管——提供各种信息安全工作必须的资源

C．系统的普通使用者——遵守日常操作规范

D．审计人员——检查安全策略是否被遵从

B

66．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?

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　幻灯片原话

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

幻灯片，ABC 都有。D 不是先进性

D

课本 226 页,CC 标准是测评标准。此标准致力于保护信息免收未授权的修改、泄露和无法使用，旨在作为评估 IT 产品和系统安全性的基础准则。

所以不能用于开发和生产过程？

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

A．全国通信标准化技术委员会(TC485)

B.全国信息安全标准化技术委员会(TC260)

C．中国通信标准化协会(CCSA)

D．网络与信息安全技术工作委员会

B

68．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：

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．I_a，V_a分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

D

69．为了不断完善一个组织的信息安全管理，应对组织的信息安全管理方法及实施情况进行独立评审，这种独立评审。

A．必须按固定的时间间隔来进行

B．应当由信息系统的运行维护人员发起

C.可以由内部审核部门或专业的第三方机构来实施

D．结束后，评审者应组织针对不符合安全策略的问题设计和实施纠正措施

C

70．以下哪一项在防止数据介质被溢用时是不推荐使用的方法：

A．禁用主机的CD驱动、USB接口等I／O设备

B．对不再使用的硬盘进行严格的数据清除

C．将不再使用的纸质文件用碎纸机粉碎

D.用快速格式化删除存储介质中的保密文件

D

71．在进行应用系统的测试时，应尽可能避免使用包含个人稳私和其它敏感信息的实际生产系统中的数据，如果需要使用时，以下哪一项不是必须做的：

A．测试系统应使用不低于生产系统的访问控制措施

B．为测试系统中的数据部署完善的备份与恢复措施

C．在测试完成后立即清除测试系统中的所有敏感数据

D．部署审计措施，记录生产数据的拷贝和使用

B

72．为了保证系统日志可靠有效，以下哪一项不是日志必需具备的特征。

A．统一而精确地的时间

B．全面覆盖系统资产

C．包括访问源、访问目标和访问活动等重要信息

D.可以让系统的所有用户方便的读取

D

73．关于信息安全事件管理和应急响应，以下说法错误的是：

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(Ⅲ级)和一般事件(Ⅳ级)

B

准备、检测、抑制、根除、恢复、跟踪

74．以下哪一项不属于信息安全工程监理模型的组成部分：

A．监理咨询支撑要素

B.控制和管理手段

C．监理咨询阶段过程

D.监理组织安全实施

D

75．以下关于灾难恢复和数据备份的理解，说法正确的是：

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 6

C.数据备份按数据类型划分可以划分为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

C

76．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：

A．项目计划书

B．质量控制计划

C．评审报告

D.需求说明书

D

77．在某网络机房建设项目中，在施工前，以下哪一项不属于监理需要审核的内容：

A．审核实施投资计划

B．审核实施进度计划

C．审核工程实施人员

D.企业资质

A

78．以下关于直接附加存储(Direct Attached Storage，DAS)说法错误的是：

A．DAS 能够在服务器物理位置比较分散的情况下实现大容量存储．是一种常用的数据存储方法

B．DAS 实现了操作系统与数据的分离，存取性能较高并且实施简单

C．DAS 的缺点在于对服务器依赖性强，当服务器发生故障时，连接在服务器上的存储设备中的数据不能被存取

D．较网络附加存储(Network Attached Storage，NAS)，DAS 节省硬盘空间，数据非常集中，便于对数据进行管理和备份

D

79．某公司在执行灾难恢复测试时．信息安全专业人员注意到灾难恢复站点的服务器的运行速度缓慢，为了找到根本愿因，他应该首先检查：

A．灾难恢复站点的错误事件报告

B．灾难恢复测试计划

C．灾难恢复计划(DRP)

D．主站点和灾难恢复站点的配置文件

A

80．以下对异地备份中心的理解最准确的是：

A．与生产中心不在同一城市

B．与生产中心距离 100 公里以上

C．与生产中心距离 200 公里以上

D．与生产中心面临相同区域性风险的机率很小

D

81．作为业务持续性计划的一部分，在进行业务影响分析(BIA)时的步骤是：

1．标识关键的业务过程

2．开发恢复优先级

3．标识关键的 IT 资源

4．表示中断影响和允许的中断时间

A． 1-3-4-2

B． 1-3-2-4

C．1－2－3－4

D． 1－4－3－2

幻灯片和课本 120 页

B

课本 120 页最上面的图

82．有关系统安全工程-能力成熟度模型(SSZ-CMM)，错误的理解是：

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

C

83．下面关于信息系统安全保障的说法不正确的是：

A．信息系统安全保障与信息系统的规划组织、开发采购、实施交付、运行维护和废弃等生命周期密切相关

B.信息系统安全保障要素包括信息的完整性、可用性和保密性 ppt 页

C．信息系统安全需要从技术、工程、管理和人员四个领域进行综合保障

D．信息系统安全保障需要将信息系统面临的风险降低到可接受的程度，从而实现其业务使命

B

84．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：

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)　　作为域维

D．测量单位是公共特征(Common Features，CF)　作为基本维

D

AC 是域维

BD 是能力维

85．下面关于信息系统安全保障模型的说法不正确的是：

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／T 20274．1-2006)中的信息系统安全保障模型将风险和策略作为基础和核心

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

C．信息系统安全保障强调的是动态持续性的长效安全，而不仅是某时间点下的安全

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

D

86．信息系统安全工程(ISSE)的一个重要目标就是在 IT 项目的各个阶段充分考虑安全因素，在 IT 项目的立项阶段，以下哪一项不是必须进行的工作：

A．明确业务对信息安全的要求

B．识别来自法律法规的安全要求

C．论证安全要求是否正确完整

D.通过测试证明系统的功能和性能可以满足安全要求

D

87．关于信息安全保障技术框架(IATF)，以下说法不正确的是：

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

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

C．允许在关键区域(例如区域边界)使用高安全级保障解决方案，确保系统安全性

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

D

88．以下哪项是对系统工程过程中“概念与需求定义”阶段的信息安全工作的正确描述?

A.应基于法律法规和用户需求，进行需求分析和风险评估，从信息系统建设的开始就综合信息系统安全保障的考虑

B．应充分调研信息安全技术发展情况和信息安全产品市场，选择最先进的安全解决方案和技术产品

C.应在将信息安全作为实施和开发人员的一项重要工作内容，提出安全开发的规范并切实落实

D．应详细规定系统验收测试中有关系统安全性测试的内容

A

89．信息安全工程监理的职责包括：

A．质量控制、进度控制、成本控制、合同管理、信息管理和协调

B．质量控制、进度控制、成本控制、合同管理和协调

C．确定安全要求、认可设计方案、监视安全态势、建立保障证据和协调

D．确定安全要求、认可设计方案、监视安全态势和协调

A

90．关于信息安全保障的概念，下面说法错误的是：

A．信息系统面临的风险和威胁是动态变化的，信息安全保障强调动态的安全理念

B．信息安全保障已从单纯的保护和防御阶段发展为集保护、检测和响应为一体的综合阶段

C.在全球互联互通的网络空间环境下，可单纯依靠技术措施来保障信息安全

D．信息安全保障把信息安全从技术扩展到管理，通过技术、管理和工程等措施的综合融合，形成对信息、信息系统及业务使命的保障

C

91．关于监理过程中成本控制，下列说法中正确的是?

A．成本只要不超过预计的收益即可

B．成本应控制得越低越好

C．成本控制由承建单位实现，监理单位只能记录实际开销

D．成本控制的主要目的是在批准的预算条件下确保项目保质按期完成

D

92．有关危害国家秘密安全的行为，包括：

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

A

93．下列关于 ISO15408 信息技术安全评估准则(简称 CC)通用性的特点，即给出通用的表

达方式，描述不正确的是_____。

A．如果用户、开发者、评估者和认可者都使用 CC 语言，互相就容易理解沟通

B．通用性的特点对规范实用方案的编写和安全测试评估都具有重要意义

C．通用性的特点是在经济全球化发展、全球信息化发展的趋势下，进行合格评定和评估结果国际互认的需要

D.通用性的特点使得 CC 也适用于对信息安全建设工程实施的成熟度进行评估

D

94．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。

A．二级以上

B．三级以上

C．四级以上

D．五级以上

B〈信息安全等级保护管理办法（公通字[2007]43 号）〉第二十二条

95．有关国家秘密，错误的是：

A．国家秘密是关系国家安全和利益的事项

B．国家秘密的确定没有正式的法定程序

C.除了明确规定需要长期保密的，其他的园家秘密都是有保密期限的

D．国家秘密只限一定范围的人知悉

B

96．在可信计算机系统评估准则(TCSEC)中，下列哪一项是满足强制保护要求的最低级别?

A．C2

B．C1

C．B2

D．B1

D

百度百科

B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

97．对涉密系统进行安全保密测评应当依据以下哪个标准?

A．BMB20-2007《涉及国家秘密的计算机信息系统分级保护管理规范》

B．BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》

C．GB17859-1999《计算机信息系统安全保护等级划分准则》

D．GB／T20271-2006《信息安全技术信息系统统用安全技术要求》

B

98．ISO／IBC27001《信息技术　安全技术　信息安全管理体系要求》的内容是基于__。

A．BS7799-1《信息安全实施细则》

B.BS7799-2《信息安全管理体系规范》

C．信息技术安全评估准则(简称 ITSEC)

D．信息技术安全评估通用标准(简称 CC)

B

99．在 GB／T 18336《信息技术安全性评估准则》中，有关保护轮廓(Protection Profile，PP)和安全目标(Security Target，ST)，错误的是：

A．PP 是描述一类产品或系统的安全要求

B．PP 描述的安全要求与具体实现无关

C．两份不同的 ST 不可能满足同一份 PP 的要求

D．ST 与具体的实现有关

C

课本 226 页。

PP 是与具体实现无关的，

100．以下哪一项不是我国国务院信息化办公室为加强信息安全保障明确提出的九项重点工作内容之一?

A.提高信息技术产品的国产化率

B．保证信息安全资金投入

C．加快信息安全人才培养

D．重视信息安全应急处理工作

A

101．最小特权是软件安全设计的基本原则，某应用程序在设计时，设计人员给出了以下四种策略，其中有一个违反了最小特权的原则，作为评审专家，请指出是哪一个?

A．软件在Linux下按照时，设定运行时使用nobody用户运行实例

B．软件的日志备份模块由于需要备份所有数据库数据，在备份模块运行时，以数据库备份操作员账号连接数据库

C．软件的日志模块由于要向数据库中的日志表中写入日志信息，使用了一个日志用户账号连接数据库，该账号仅对日志表拥有权限

D.为了保证软件在Windows下能稳定的运行，设定运行权限为system，确保系统运行正常，不会因为权限不足产生运行错误

D

102．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，请指出大家提的建议中不太合适的一条?

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识

C.要求软件开发商使用Java而不是ASP作为开发语言，避免产生SQL注入漏洞

D．要求软件开发商对软件进行模块化设计，各模块明确输入和输出数据格式，并在使用前对输入数据进行校验

C

103．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．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

A

104．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日志共享，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?

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

D

105．如图 1 所示，主机 A 向主机 B 发出的数据采用 AH 或 ESP 的传输模式对流量进行保护时，主机 A 和主机 B 的 IP 地址在应该在下列哪个范围?

A．10．0．0．0～10．255．255．255

B．172．16．0．0～172．31．255．255

C、192．168．0．0～192．168．255．255

D.不在上述范围内

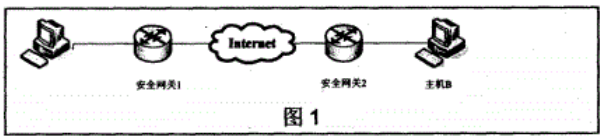


图 1

传输模式不能修改 IP

D

Class A 10.0.0.0-10.255.255.255

默认子网掩码:255.0.0.0

Class B 172.16.0.0-172.31.255.255

默认子网掩码:255.255.0.0

Class C 192.168.0.0-192.168.255.255

默认子网掩码:255.255.255.0

106．某电子商务网站最近发生了一起安全事件，出现了一个价值 1000 元的商品用 1 元被买走的情况，经分析是由于设计时出于性能考虑，在浏览时使用 Http 协议，攻击者通过伪造数据包使得向购物车添加商品的价格被修改．利用此漏洞，攻击者将价值 1000 元的商品以 1 元添加到购物车中，而付款时又没有验证的环节，导致以上问题，对于网站的这个问题原因分析及解决措施。最正确的说法应该是?

A．该问题的产生是由于使用了不安全的协议导致的，为了避免再发生类似的闯题，应对全网站进行安全改造，所有的访问都强制要求使用 https

B．该问题的产生是由于网站开发前没有进行如威胁建模等相关工作或工作不到位，没有找到该威胁并采取相应的消减措施

C．该问题的产生是由于编码缺陷，通过对网站进行修改，在进行订单付款时进行商品价格验证就可以解决

D．该问题的产生不是网站的问题，应报警要求寻求警察介入，严惩攻击者即可

B

107．针对软件的拒绝服务攻击是通过消耗系统资源使软件无法响应正常请求的一种攻击方式，在软件开发时分析拒绝服务攻击的威胁，以下哪个不是需要考虑的攻击方式：

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

B．攻击者利用软件脚本使用多重嵌套查询，在数据量大时会导致查询效率低，通过发送大量的查询导致数据库响应缓慢

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

D.攻击者买通了 IDC 人员，将某软件运行服务器的网线拔掉导致无法访问

D

108．以下哪个选项不是防火墙提供的安全功能?

A．IP 地址欺骗防护

B．NAT

C．访问控制

D．SQL 注入攻击防护

D

109．以下关于可信计算说法错误的是：

A. 可信的主要目的是要建立起主动防御的信息安全保障体系

B. 可信计算机安全评价标准(TCSEC)中第一次提出了可信计算机和可信计算基的概念

C. 可信的整体框架包含终端可信、终端应用可信、操作系统可信、网络互联可信、互联网交易等应用系统可信

D. 可信计算平台出现后会取代传统的安全防护体系和方法

D

110.Linux 系统对文件的权限是以模式位的形式来表示,对于文件名为 test 的一个文件,属于 admin 组中 user 用户，以下哪个是该文件正确的模式表示?

A.rwxr-xr-x3 user admin 1024 Sep 13 11：58 test

B.drwxr-xr-x 3 user admin 1024 Sep 13 11：58 test

C. rwxr-xr-x 3 admin user 1024 Sep 13 11：58 test

D. drwxr-xr-x 3 admin user1024 Sep 13 11：58 test

A

111. Apache Web 服务器的配置文件一般位于/usr / local / apache / conf 目录，其中用来控制用户访问 Apache 目录的配置文件是：

A.httpd. conf

B. srL conf

C. access. conf

D. inetd. conf

A

112. 应用软件的数据存储在数据库中，为了保证数据安全，应设置良好的数据库防护策略，以下不属于数据库防护策略的是?

A. 安装最新的数据库软件安全补丁

B. 对存储的敏感数据进行安全加密

C. 不使用管理员权限直接连接数据库系统

D. 定期对数据库服务器进行重启以确保数据库运行良好

D

113. 下列哪项内容描述的是缓冲区溢出漏洞?

A.通过把 SQL 命令插入到 web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令

B．攻击者在远程 WEB 页面的 HTML 代码中插入具有恶意目的的数据，用户认为该页面是可信赖的，但是当浏览器下载该页面，嵌入其中的脚本将被解释执行。

C．当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量溢出的数据覆盖在合法数据上

D．信息技术、信息产品、信息系统在设计、实现、配置、运行等过程中，有意或无意产生的缺陷

C

114．对恶意代码的预防，需要采取增强安全防范策略与意识等措施，关于以下预防措施或意识，说法错误的是：

A．在使用来自外部的移动介质前，需要进行安全扫描

B．限制用户对管理员权限的使用

C.开放所有端口和服务，充分使用系统资源

D．不要从不可信来源下载或执行应用程序

C

115．安全专家在对某网站进行安全部署时，调整了 Apache 的运行权限，从 root 权限降低为 nobody 用户，以下操作的主要目的是：

A．为了提高 Apache 软件运行效率

B．为了提高 Apache 软件的可靠性

C.为了避免攻击者通过 Apache 获得 root 权限

D．为了减少 Apache 上存在的漏洞

C

116．下列关于计算机病毒感染能力的说法不正确的是：

A．能将自身代码注入到引导区

B．能将自身代码注入到扇区中的文件镜像

C．能将自身代码注入文本文件中并执行

D．能将自身代码注入到文档或模板的宏中代码

C

117．以下哪个是恶意代码采用的隐藏技术：

A．文件隐藏

B．进程隐藏

C．网络连接隐藏

D．以上都是

D

118．通过向被攻击者发送大量的 ICMP 回应请求，消耗被攻击者的资源来进行响应，直至被攻击者再也无法处理有效的网络信息流时，这种攻击称之为：

A．Land 攻击

B．Smurf 攻击

C．Ping of Death 攻击

D.ICMP Flood

D

119．以下哪个拒绝服务攻击方式不是流量型拒绝服务攻击

A．Land

B．UDP Flood

C．Smurf

D.teardrop

D

120．传输控制协议(TCP)是传输层协议，以下关于 TCP 协议的说法，哪个是正确的?

A．相比传输层的另外一个协议 UDP，TCP 既提供传输可靠性，还同时具有更高的效率，因此具有广泛的用途

B．TCP 协议包头中包含了源 IP 地址和目的 IP 地址，因此 TCP 协议负责将数据传送到正确的主机

C．TCP 协议具有流量控制、数据校验、超时重发、接收确认等机制，因此 TCP 协议能完全替代 IP 协议

D.TCP 协议虽然高可靠，但是相比 UDP 协议机制过于复杂，传输效率要比 UDP 低

D

121．以下关于 UDP 协议的说法，哪个是错误的?

A．UDP 具有简单高效的特点，常被攻击者用来实施流量型拒绝服务攻击

B．UDP 协议包头中包含了源端口号和目的端口号，因此 UDP 可通过端口号将数据包送达正确的程序

C．相比 TCP 协议，UDP 协议的系统开销更小，因此常用来传送如视频这一类高流量需求

的应用数据

D. UDP 协议不仅具有流量控制，超时重发等机制，还能提供加密等服务，因此常用来传输如视频会话这类需要隐私保护的数据

D

122. 有关项目管理，错误的理解是：

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

B

123. 近年来利用 DNS 劫持攻击大型网站恶性攻击事件时有发生，防范这种攻击比较有效的方法是?

A. 加强网站源代码的安全性

B. 对网络客户端进行安全评估

C.协调运营商对域名解析服务器进行加固

D. 在网站的网络出口部署应用级防火墙

C

124. 关于源代码审核，下列说法正确的是：

A. 人工审核源代码审校的效率低，但采用多人并行分析可以完全弥补这个缺点

B. 源代码审核通过提供非预期的输入并监视异常结果来发现软件故障，从而定位可能导致安全弱点的薄弱之处

C. 使用工具进行源代码审核，速度快，准确率高，已经取代了传统的人工审核

D.源代码审核是对源代码检查分析，检测并报告源代码中可能导致安全弱点的薄弱之处

D

125. 在戴明环(PDCA)模型中，处置(ACT)环节的信息安全管理活动是：

A. 建立环境

B. 实施风险处理计划

C．持续的监视与评审风险

D.持续改进信息安全管理过程

D

126．信息系统的业务特性应该从哪里获取?

A．机构的使命

B．机构的战略背景和战略目标

C.机构的业务内容和业务流程

D．机构的组织结构和管理制度

C

127．在信息系统设计阶段，“安全产品选择”处于风险管理过程的哪个阶段?

A．背景建立

B．风险评估

C．风险处理

D．批准监督

C

128．以下关于“最小特权”安全管理原则理解正确的是：

A．组织机构内的敏感岗位不能由一个人长期负责

B．对重要的工作进行分解，分配给不同人员完成

C.一个人有且仅有其执行岗位所足够的许可和权限

D．防止员工由一个岗位变动到另一个岗位，累积越来越多的权限

C

129．以下哪一项不属于常见的风险评估与管理工具：

A．基于信息安全标准的风险评估与管理工具

B．基于知识的风险评估与管理工具

C.基于模型的风险评估与管理工具

D．基于经验的风险评估与管理工具

D

幻灯片上有，没有第四个

130．以下说法正确的是：

A．验收测试是由承建方和用户按照用户使用手册执行软件验收

B．软件测试的目的是为了验证软件功能是否正确

c．监理工程师应按照有关标准审查提交的测试计划，并提出审查意见

D．软件测试计划开始于软件设计阶段，完成于软件开发阶段

C

131．信息系统安全保护等级为3级的系统，应当()年进行一次等级测评?

A．0．5

B.1

C．2

D．3

B

132.国家科学技术秘密的密级分为绝密级、机密级、秘密级，以下哪项属于绝密级的描述?

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

D

133.关于我国加强信息安全保障工作的总体要求，以下说法错误的是：

A．坚持积极防御、综合防范的方针

B．重点保障基础信息网络和重要信息系统安全

C．创建安全健康的网络环境　　选项来自于课本201页第二段内容

D．提高个人隐私保护意识

D

134.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：

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．可委托同一专业测评机构完成等级测评和风险评估工作，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

C

做等级测评时，必须有风险评估报告。

135.某单位信息安全岗位员工，利用个人业余时阀，在社交网络平台上向业内同不定期发布信息安全相关知识和前沿动态资讯，这一行为主要符合以下哪一条注册信息安全专业人员（CISP）职业道德准则：

A．避免任何损害CISP声誉形象的行为

B．自觉维护公众信息安全，拒绝并抵制通过计算机网络系统泄露个人隐私的行为

C．帮助和指导信息安全同行提升信息安全保障知识和能力

D．不在公众网络传播反动、暴力、黄色、低俗信息及非法软件

C

136.信息安全保障技术框架(Information Assurance Technical Framework，IATF)由美国国家安全局(NSA)发布，最初目的是为保障美国政府和工业的信息基础设施安全提供技术指南，其中，提出需要防护的三类“焦点区域”是：

A．网络和基础设施区域边界重要服务器

B．网络和基础设施区域边界计算环境

C．网络机房环境　网络接口计算环境

D．网络机房环境　网络接口重要服务器

B

137.以下哪一项不是我国信息安全保障的原则：

A．立足国情，以我为主，坚持以技术为主

B．正确处理安全与发展的关系，以安全保发展，在发展中求安全

C．统筹规划，突出重点，强化基础性工作

D．明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息安全保障体系

A

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

A．健全国家信息安全组织与管理体制机制，加强信息安全工作的组织保障

B．建设信息安全基础设施，提供国家信息安全保障能力支撑

C．建立信息安全技术体系，实现国家信息化发展的自主创新

D．建立信息安全人才培养体系，加快信息安全学科建设和信息安全人才培养

C

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

A．信息系统安全必须遵循的相关法律法规，国家以及金融行业安全标准

B．信息系统所承载该银行业务正常运行的安全需求

C．消除或降低该银行信息系统面临的所有安全风险

D．该银行整体安全策略

C

140.下列选项中，哪个不是我国信息安全保障工作的主要内容：

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，尽快建立和完善我国信息安全标准体系

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

B

141.关于信息安全管理，说法错误的是：

A．信息安全管理是管理者为实现信息安全目标(信息资产的 CIA 等特性，以及业务运作的持续)而进行的计划、组织、指挥、协调和控制的一系列活动。

B．信息安全管理是一个多层面、多因素的过程，依赖于建立信息安全组织、明确信息安全角色及职责、制定信息安全方针策略标准规范、建立有效的监督审计机制等多方面非技术性的努力。

C．实现信息安全，技术和产品是基础，管理是关键。

D．信息安全管理是人员、技术、操作三者紧密结合的系统工程，是一个静态过程。

D

142.以下哪个选项不是信息安全需求的来源?

A．法律法规与合同条约的要求

B．组织的原则、目标和规定

C．风险评估的结果

D．安全架构和安全厂商发布的病毒、漏洞预警

D

143.下列关于信息系统生命周期中实施阶段所涉及主要安全需求描述错误的是：

A．确保采购定制的设备、软件和其他系统组件满足已定义的安全要求

B．确保整个系统已按照领导要求进行了部署和配置

C．确保系统使用人员已具备使用系统安全功能和安全特性的能力

D．确保信息系统的使用已得到授权

B

144.下列关于信息系统生命周期中安全需求说法不准确的是：

A．明确安全总体方针，确保安全总体方针源自业务期望

B．描述所涉及系统的安全现状，提交明确的安全需求文档

C．向相关组织和领导人宣贯风险评估准则

D．对系统规划中安全实现的可能性进行充分分析和论证

C

课本69页。第二章节第1小节原文

145.小张在某单位是负责事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，小张主要负责讲解风险评估工作形式，小张认为：1．风险评估工作形式包括：自评估和检查评估；2．自评估是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行风险评估；3．检查评估是信息系统上级管理部门组织或者国家有关职能部门依法开展的风险评估；4．对信息系统的风险评估方式只能是“自评估”和“检查评估”中的一个，非此即彼，请问小张的所述论点中错误的是哪项：

A．第一个观点

B．第二个观点

C．第三个观点

D．第四个观点

D

146.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

B

147.风险评估工具的使用在一定程度上解决了手动评估的局限性，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛使用，根据在风险评估过程中的主要任务和作用愿理，风险评估工具可以为以下几类，其中错误的是：

A．风险评估与管理工具

B．系统基础平台风险评估工具

C．风险评估辅助工具

D．环境风险评估工具

D 课本 78 页

148.为了解风险和控制风险，应当及时进行风险评估活动，我国有关文件指出：风险评估的工作形式可分为自评估和检查评估两种，关于自评估，下面选项中描述错误的是()。

A．自评估是由信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估

B．自评估应参照相应标准、依据制定的评估方案和评估准则，结合系统特定的安全要求实施

C．自评估应当是由发起单位自行组织力量完成，而不应委托社会风险评估服务机构来实施

D．周期性的自评估可以在评估流程上适当简化，如重点针对上次评估后系统变化部分进行

C

149.信息安全风险评估是信息安全风险管理工作中的重要环节，在国家网络与信息安全协调小组发布的《关于开展信息安全风险评估工作的意见》(国信办(2006)5 号)中，风险评估分为自评估和检查评估两种形式，并对两种工作形式提出了有关工作原则和要求，下面选项

中描述正确的是()。

A．信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充

B．信息安全风险评估应以检查评估为主，自评估和检查评估相互结合、互为补充

C．自评估和检查评估是相互排斥的，单位应慎重地从两种工作形式选择一个，并长期使用

D．自评估和检查评估是相互排斥的，无特殊理由的单位均应选择检查评估，以保证安全效果

A

150.某单位的信息安全主管部门在学习我国有关信息安全的政策和文件后，认识到信息安全风险评估分为自评估和检查评估两种形式。该部门将有关检查评估的特点和要求整理成如下四条报告给单位领导，其中描述错误的是()。

A．检查评估可依据相关标准的要求，实施完整的风险评估过程；也可在自评估的基础上，对关键环节或重点内容实施抽样评估

B．检查评估可以由上级管理部门组织，也可以由本级单位发起，其重点是针对存在的问题进行检查和评测

C．检查评估可以由上级管理部门组织，并委托有资质的第三方技术机构实施

D．检查评估是通过行政手段加强信息安全管理的重要措施，具有强制性的特点

B

151.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值为 200 万元人民币，暴露系数(ExposureFactor，EF)是 25%，年度发生率(Annualized Rate ofOccurrence,ARO)为 0.1,那么小王计算的年度预期损失(Annualized Loss Expectancy，ALE)应该是()。

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

A

152.规范的实施流程和文档管理，是信息安全风险评估结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。

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

A

153. 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。

A．风险评估准备

B．风险要素识别

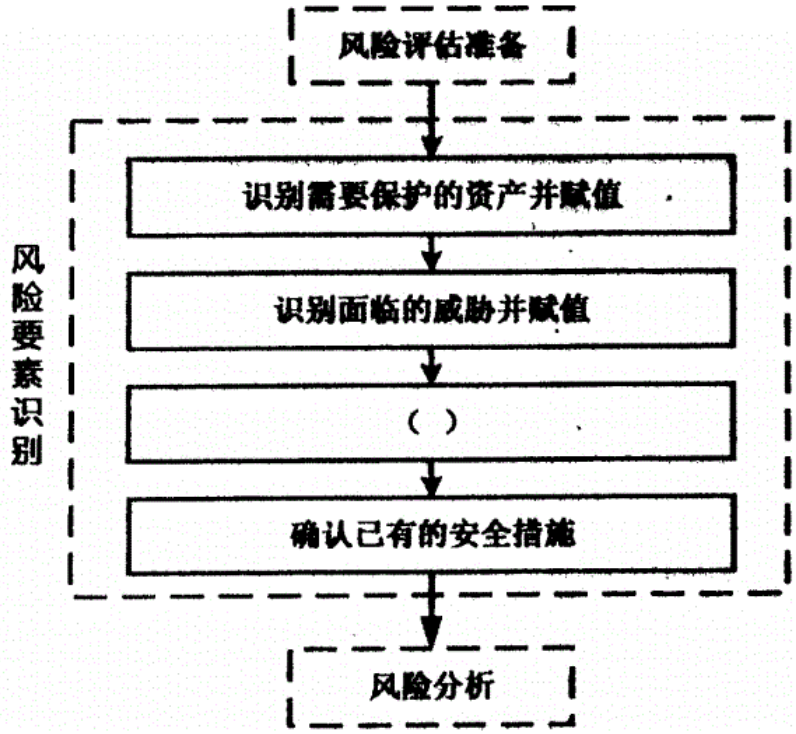
C．风险分析

D．风险结果判定

B

74 页”风险要素识别”部分-资产识别与赋值

154.风险要素识别是风险评估实施过程中的一个重要步骤，小李将风险要素识别的主要过程使用图形来表示，如下图所示，请为图中空白框处选择一个最合适的选项()。



A．识别面临的风险并赋值

B．识别存在的脆弱性并赋值

C．制定安全措施实施计划

D．检查安全措施有效性

B

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

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.《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》，主要包括风险评估参考标准、采用的风险分析方法、风险计算

方法、资产分类标准、资产分类准则等内容

C

课本 74 页

156.文档体系建设是信息安全管理体系(ISMS)建设的直接体现，下列说法不正确的是：

A．组织内的信息安全方针文件、信息安全规章制度文件、信息安全相关操作规范文件等文档是组织的工作标准，也是 ISMS 审核的依据

B．组织内的业务系统日志文件、风险评估报告等文档是对上一级文件的执行和记录，对这些记录不需要保护和控制

C.组织在每份文件的首页，加上文件修订跟踪表，以显示每一版本的版本号、发布日期、编写人、审批人、主要修订等内容

D．层次化的文档是 ISMS 建设的直接体现，文档体系应当依据风险评估的结果建立

B

157.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-CMM)定义了 3 个风险过程：评价威胁，评价脆弱性，评价影响。4 个

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。 相互联系的

A

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

A．在异地建立备份机房时，设计时应与主用机房等级相同

B．由于高端小型机发热量大，因此采用活动地板上送风，下回风的方式

《电子信息系统机房设计规范》(GB50174-2008)第 9 页

送风方式有 3 种:下送上回,上送上回,侧送侧回

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

D．A 级主机房应设置洁净气体灭火系统

B

159.在工程实施阶段，监理机构依据承建合同、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。

A．功能性

B．可用性

C．保障性

D．符合性

D

160.以下系统工程说法错误的是：

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．系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法

D．系统工程是一种方法论

A

161.系统安全工程-能力成熟度模型(Systems Security Engineoring-Capability maturity model，SSE-CMM)定义的包含评估威胁、评估脆弱性、评估影响和评估安全风险的基本过程领域是：

A．风险过程

B．工程过程

C．保证过程

D．评估过程

A　P172

162.有关系统安全工程-能力成熟度模型(SSE-CMM)中的通用实施(Generic Practices，GP)，错误的理解是：

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(Process Areas，PA)的活动而非所有PA的活动

课本170页内容，GP是通用实施，适用于所有过程区域。

C．在工程实施时，GP应该作为基本实施(Base，Practices，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

B

163.以下关于信息安全工程说法正确的是：

A.信息化建设中系统功能的实现是最重要的

B．信息化建设可以先实施系统，而后对系统进行安全加固

C．信息化建设中在规划阶段合理规划信息安全，在建设阶段要同步实施信息安全建设

D．信息化建设没有必要涉及信息安全建设

C

164.关于业务连续性计划（bcp）以下说法最恰当的是：

A. 组织为避免所有业务功能因重大事件而中断，减少业务风险而建立的控制过程；

B. 组织为避免关键业务功能因重大事件而中断，减少业务风险而建立的一个控制过程；

c. 组织为避免所有业务功能因各种事件而中断，减少业务风险而建立的一个控制过程；

D. 组织为避免信息系统功能因各种事件而中断，减少信息系统而建立的一个控制过程。

B

165.组织建立业务连续性计划（BCP)的作用包括：

A. 在遭遇灾难事件时，能够最大限度地保护组织数据的实时性，完整性和一致性；，

B. 提供各种恢复策略选择，尽量减小数据损失和恢复时间，快速恢复操作系统、应用和数据；

C. 保证发生各种不可预料的故障、破坏性事故或灾难情况时，能够持续服务，确保业务系统的不间断运行，降低损失；

D. 以上都是。

D

166.业务系统运行中异常错误处理合理的方法是：

A. 让系统自己处理异常

B. 调试方便，应该让更多的错误更详细的显示出来

c. 捕获错误，并抛出前台显示

D. 捕获错误，只显示简单的提示信息，或不显示任何信息

D

167.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：

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

D

168.以下哪项不是应急响应准备阶段应该做的？

A.确定重要资产和风险，实施针对风险的防护措施

B.编制和管理应急响应计划

C.建立和训练应急响应组织和准备相关的资源

D.评估时间的影响范围，增强审计功能、备份完整系统

D

169.关于秘钥管理，下列说法错误的是：

A. 科克霍夫原则指出算法的安全性不应基于算法的保密，而应基于秘钥的安全性

B. 保密通信过程中，通信方使用之前用过的会话秘钥建立会话，不影响通信安全

c.秘钥管理需要考虑秘钥产生、存储、备份、分配、更新、撤销等生命周期过程的每一个环节

D.在网络通信中。通信双方可利用 Diffie-Hellman 协议协商出会话秘钥

B

170.以下属于哪一种认证实现方式：用户登录时，认证服务器（Authentication Server，AS)产生一个随机数发送给用户，用户用某种单向算法将自己的口令、种子秘钥和随机数混合计算后作为一次性口令，并发送给 AS,AS 用同样的防腐计算后，验证比较两个口令即可验证用户身份。

A. 口令序列

B. 时间同步

C.挑战/应答

D.静态口令

C

171.部署互联网协议安全虚拟专用网（Internet protocolSecurityvirtualPrivate NetworkIPsecVPN）时。以下说法正确的是：

A. 配置 MD5 安全算法可以提供可靠地数据加密 1

B. 配置 AES 算法可以提供可靠的数据完整性验证 1

c. 部署 IPsecVIPN 网络时，需要考虑 IP 地址的规划，尽量在分支节点使用可以聚合的 IP 地址段，来减少 IPsec 安全关联（Security Authentication，SA)资源的消耗

D. 报文验证头协议（Authentication Header，AH)可以提供数据机密性 1

C

172：在对某面向互联网提供服务的某应用服务器的安全检测中发现，服务器上开放了以下几个应用，除了一个应用外其他应用都存在明文传输信息的安全问题，作为一名检测人员，你需要告诉用户对应用进行安全整改以外解决明文传输数据的问题，以下哪个应用已经解决了明文传输数据问题：

A. SSH

B. HTTP

C. FTP

D. SMTP

A

173：某单位发生的管理员小张在繁忙的工作中接到了一个电话，来电者：小张吗？我是科技处李强，我的邮箱密码忘记了，现在打不开邮件，我着急收个邮件，麻烦你先帮我把密码改成 123，我收完邮件自己修改掉密码。热心的小张很快的满足了来电考的要求。后来，李强发现邮箱系统登录异常。请问以下说法哪个是正确的？

A，小张服务态度不好，如果把李强的邮件收下来亲自交给李强就不会发生这个问题

B，事件属于服务器故障，是偶然事件，应向单位领导申请购买新的服务器。

C，单位缺乏良好的密码修改操作流程或者小张没有按操作流程工作

D，事件属于邮件系统故障，是偶然事件，应向单位领导申请升级邮件服务软件

C

174，以下哪个属性不会出现在防火墙的访问控制策略配置中？

A. 本局域网内地址

B. 百度服务器地址

C. HTTP 协议

D. 病毒类型

D

175，S 公司在全国有 20 个分支机构，总部有 10 台服务器、200 个用户终端，每个分支机构都有一台服务器、100 个左右用户终端，通过专网进行互联互通。公司招标的网络设计方

案中，四家集成商给出了各自的 IP 地址规划和分配的方法，作为评标专家，请给 S 公司选出设计最合理的一个：

A．总部使用服务器、用户终端统一作用 10.0.1.X、各分支机构服务器和用户终端使用 192.168.2.X~192.168.20.X

B．总部使用服务器使用 10.0.1.1~11、用户终端使用 10.0.1.12~212，分支机构 IP 地址随意确定即可

C．总部服务器使用 10.0.1.X、 用户终端根据部门划分使用 10.0.2.X、 每个分支机构分配两个 A 类地址段，一个用做服务器地址段、另外一个做用户终端地址段

D．因为通过互联网连接，访问的是互联网地址，内部地址经 NAT 映射，因此 IP 地址无需特别规划，各机构自行决定即可

A

176．windows 文件系统权限管理作用访问控制列表（Access Control List.ACL）机制，以下哪个说法是错误的：

A．安装 Windows 系统时要确保文件格式使用的是 NTFS ，因为 Windows 的 ACL 机制需要 NTFS 文件格式的支持

B．由于 windows 操作系统自身有大量的文件和目录，因此很难对每个文件和目录设置严格的访问权限 ，为了作用上的便利，Windows 上的 ACL 存在默认设置安全性不高的问题

C．windows 的 ACL 机制中，文件和文件夹的权限是与主体进行关联的，即文件夹和文件的访问权限信息是写在用户数据库中

D．由于 ACL 具有很好的灵活性，在实际使用中可以为每一个文件设定独立的用户的权限

C

177：某 linux 系统由于 root 口令过于简单，被攻击者猜解后获得了 root 口令，发现被攻击后，管理员更改了 root 口令，并请安全专家对系统进行检测，在系统中发现有一个文件的权限如下 -r-s--x--x 1 test tdst 10704 apr 15 2002/home/test/sh 请问以下描述哪个是正确 的：

A．该文件是一个正常文件，test 用户使用的 shell,test 不能读该文件，只能执行

B．该文件是一个正常文件，是 test 用户使用的 shell,但 test 用户无权执行该文件

C．该文件是一个后门程序 ，该文件被执行时，运行身份是 root ,test 用户间接获得了 root 权限

D．该文件是一个后门程序 ，由于所有者是 test ，因此运行这个文件时文件执行权限为

test

C

178．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，将威胁分为六类，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？

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漏，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信息

D

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

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

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

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

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

D

180．微软提出了 STRIDE 模型，其中 R 是 Repudiation(抵赖)的缩写，关于此项安全要求下面描述错误的是

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就属于 R 威胁

B.解决 R 威胁，可以选择使用抗抵赖性服务技术来解决，如强认证、数字签名、安全审

计等技术措施

C.R 威胁是 STRIDE 六种威胁中第三严重的威胁，比 D 威胁和 E 威胁的严重程度更高

D.解决 R 威胁，也应按照确定建模对象、识别威胁、评估威胁以及消减威胁等四个步骤来进行

C

181．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陆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

C

182．以下关于威胁建模流程步骤说法不正确的是

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，威胁就是漏洞。

D

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

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

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

C.渗透测试应当经过方案制定、信息收集、漏洞利用、完成渗透测试报告等步骤

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

D

184．某政府机构拟建设一机房，在工程安全监理单位参与下制定了招标文件，项目分二期，一期目标为年底前实现系统上线运营，二期目标为次年上半年完成运行系统风险的处理，招标文件经管理层审批后发布。就此工程项目而言，以下正确的是

A.此项目将项目目标分解为系统上线运营和运行系统风险处理分期实施，具有合理性和可行性

B.在工程安全监理的参与下，确保了此招标文件的合理性

C.工程规划不符合信息安全工程的基本原则

D.招标文件经管理层审批，表明工程目标符合业务发展规划

C

185．有关系统工程的特点，以下错误的是

A.系统工程研究问题一般采用先决定整体框架，后进入详细设计的程序

B.系统工程的基本特点，是需要把研究对象解构为多个组成部分分别独立研究

互相联系，不能独立研究

SSECMM 的知识点

C.系统工程研究强调多学科协作，根据研究问题涉及到的学科和专业范围，组成一个知识结构合理的专家体系

D.系统工程研究是以系统思想为指导，采取的理论和方法是综合集成各学科、各领域的理论和方法

b

186．有关能力成熟度模型（CMM）错误的理解是

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”

A

187．在提高阿帕奇系统(Apache HTTP Server)系统安全性时，下面哪项措施不属于安全配置内容()？

A．不在 Windows 下安装 Apache，只在 Linux 和 Unix 下安装

B．安装 Apache 时，只安装需要的组件模块

C．不使用操作系统管理员用户身份运行 Apache，而是采用权限受限的专用用户账号来运行

D．积极了解 Apache 的安全通告，并及时下载和更新

A

188. 某公司开发了一个游戏网站，但是由于网站软件存在漏洞，在网络中传输大数据包时总是会丢失一些数据，如一次性传输大于 2000 个字节数据时，总是会有 3 到 5 个字节不能传送到对方，关于此案例，可以推断的是（）

A 该网站软件存在 保密性方面安全问题

B 该网站软件存在完整性方面安全问题

C 该网站软件存在 可用性方面安全问题

D 该 网站软件存在 不可否认性方面安全问题

B

189. 信息安全保障是网络时代各国维护国家安全和利益的首要任务，以下哪个国家最早将网络安全上长升为国家安全战略，并制定相关战略计划。

A 中国

B 俄罗斯

C 美国

D 英国

C

190. 我国党和政府一直重视信息安全工作，我国信息安全保障工作也取得了明显成效，关于我国信息安全实践工作，下面说法错误的是（）

A 加强信息安全标准化建设 ，成立了“全国信息安全标准化技术委员会”制订和发布了大批信息安全技术，管理等方面的标准。

B，重视信息安全应急处理工作，确定由国家密码管理局牵头成立 “国家网络应急中心”推动了应急处理和信息通报技术合作工作进展

C 推进信息安全等级保护工作，研究制定了多个有关信息安全等级保护的规范和标准，重点保障了关系国定安全，经济命脉和社会稳定等方面重要信息系统的安全性

D 实施了信息安全风险评估工作，探索了风险评估工作的基本规律和方法，检验并修改

完善了有关标准，培养和锻炼了人才队伍

B

191. 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，并严格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 信息安全需求是安全方案设计和安全措施实施的依据

B 信息安全需求应当是从信息系统所有者（用户）的角度出发，使用规范化，结构化的语言来描述信息系统安全保障需求

C 信息安全需求应当基于信息安全风险评估结果，业务需求和有关政策法规和标准的合规性要求得到

信息安全需求来至于：复合性要求，业务需求，风险

信息系统安全评测包括信息系统风险评估、信息系统等级保护测评，信息系统安全保障测评。

信息系统安全评测的目的是提供产品的安全性证据。

D 信息安全需求来自于该公众服务信息系统的功能设计方案

现有需求，再有功能。

D

192. 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工作的主要原则？

A More《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》

C

193. 在以下标准中，属于推荐性国家标准的是？

A.GB/T XXXX.X-200X

B.GB XXXX-200X

C.DBXX/T XXX-200X

D.GB/Z XXX-XXX-200X

A

194. 微软 slm 将软件开发生命周期制分为七个阶段，并列出了十七项重要的安全活动。其中“弃用不安全的函数”属于（）的安全活动

A.要求（rapuiroments）阶段

B.设计（design）阶段

C.实施（lmplenpentation）阶段

D.验证（venifcation）阶段

C

195. 由于频繁出现燃机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开发知识培训

B.要求增加软件源代码审核环节，加强对软件代码的安全性审查

C.要求统一采用 Windows8 系统进行开发，不能采用之前的 Windows 版本

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

C

196. 金女士经常通过计算机网络购物，从安全角度看，下面哪项是不好的操作

a、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

b、为计算机安装具有良好声誉的安全防范软件包括病毒查杀、安

c、在 ie 的配置中，设置只能下载和安装经过签名的、安全的 acti

d、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

D

197. 关于源代码审核，描述正确的是（）

A.源代码审核过程遵循信息安全保障技术框架模型，在执行时应一步一步严格执行

B.源代码审核有利于发现软件编码中存在的安全问题，相关的审核工具既有商业 开源工具

C.源代码审核如果想要有效率高，则主要要依赖人工审核而不是工具审核，因为人工智能的，需要人的脑袋来判断

D.源代码审核能起到很好的安全保证作用，如果执行了源代码审核，则不需要安全测试

B

198. 微软提出了 STRIDE 模型，其中 R 是 Repudiation(抵赖)的缩写，关于此项错误的事

是（）

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 R 威胁

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”威胁也属于 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

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

D

199. 某单位开发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性测试，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，以下哪条是渗透性的优势？

A.渗透测试使用人工进行测试，不依赖软件，因此测试更准确

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期产生的漏洞

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

C

200. 以下关于软件安全测试说法正确 的是（）

A.软件安全测试就是黑盒测试

B.FUZZ 测试是经常采用的安全测试方法之一

C.软件安全测试关注的是软件的功能

D.软件安全测试可以发现软件中产生的所有安全问题

B

201. 在工程实验阶段，什么机构依据承建合同，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

A 功能性

B 可用性

C 保障性

D 符合性

D

202. 信息安全工程作为信息安全保障的重要组成部门，主要是为了解决：

A.信息系统的技术架构安全问题

B.信息系统组成部门的组件安全问题

C.信息系统生命周期的过程安全问题

D.信息系统运行维护的安全管理问题

C

203. 有关系统安全工程 -能力成熟度模型 （SSE-CMM)中基本实施 （Base Rractes）正确的理解是 ：

A.BP 不限定于特定的方法工具，不同业务背景中可以使用不同的方法

不限工具，必须按步骤执行

B.BP 不是根据广泛的现有资料，实施和专家意见综合得出的

C.BP 不代表信息安全工程领域的最佳实践

代表最佳实践

D.BP 不是过程区域 （Process Arebs ，PA ）的强制项

是强制项

A

204. 在使用系统工具安全工程能力成熟度模型 （SSE-CMM） 对一个组织的安全工程能力成熟度进行测量时，有关测量结果，错误理解的是

A.如果该组织在执行某个特定的过程区域具备了一个特定级别的部门公共特征时，这个组织过程的能力成熟度未达到级别

B.如果该组织过个工程区域 （Process Areas PA)具备了 定义标准过程 ，执行已定义的过程， 两个公共特征 ，对此工程区域的能力成熟度级别达到 3 级充分定义级

幻灯片中，有 3 个公共特征。

C.如果某个区域过程（Prpcess Areas PA ）包含的 4 个基本措施（Base Pracbces， BP）执行此 BP 时执行了 3 个 BP 此过程区域的能力成熟度级别为 0

D.组织在不同的过程区域能力成熟度可能处于不同级别上

B

205. 具有行政法律责任强制力的安全管理规定和安全规范制度包括

A.安全事件 （包括安全事故）报告制度

B.安全等级保护制度

C.信息体统安全监控

D.安全专用产品销售许可证制度

A. 1.2.4

B.2.3

C.2.3.4

D.1.2.3

A

206. 某单位在实施风险评估时，按照规范形成了若干文档，其中，（）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

A.《风险评估方法》，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》，主要经验检查确认后的已有技术和管理方面安全措施等内容

D

207. 层次化的文档是信息安全管理体系《information Securlty Management System. ISMS》建设的直接体系，也 ISMS 建设的成果之一，通常将 ISMS 的文档结构规划为 4 层金字塔结构，那么，以下选项（）应放入到一级文件中.

A.《风险评估报告》

B.《人力资源安全管理规定》

C.《ISMS 内部审核计划》

D.《单位信息安全方针》

D

208. 信息安全管理体系（information Securlty Management System. ISMS）的内部审核和管理审核是两项重要的管理活动，关于这两者，下面描述错误的是（）

A、内部审核和管理评审都很重要，都是促进 ISMS 持续改进的重要动力，也都应当按照一定的周期实施

B、内部审核的实施方式多采用文件审核和现场审核的形式，而管理评审的实施方式多采

用召开管理评审会议的形式进行

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

由组织的管理层管理

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

c

209. 信息安全管理体系（information Securlty Management System. 简称 ISMS）的实施和运行 ISMS 阶段，是 ISMS 过程模型的实施阶段，下面给出了一些备选的活动，选项（）描述了在此阶段组织应进行的活动。

①制定风险处理计划②实施风险处理计划③开发有效性测量程序④实施培训和意识教育计划⑤管理 ISMS 的运行⑥管理 ISMS 的资源⑦执行检测事态和响应事件的程序⑧实施内部审核⑨实施风险再评估

A.①②③④⑤⑥

B.①②③④⑤⑥⑦

C.①②③④⑤⑥⑦⑧

D.①②③④⑤⑥⑦⑧⑨

B

幻灯片的内容，7 个部分

210. 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（）

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

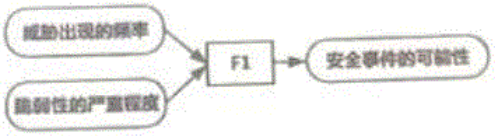
D.资产的价值无法估计

C

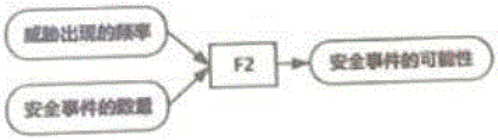
211. 小陈自学了信息安全风险评估的相关理论知识后，根据风险分析阶段的工作内容和计量方法只是，绘制了如下四张图，图中 F1、F2、F3、F4 分别代表某种计算函数，四组图中，计算关系表达正确的是（）

幻灯片内容

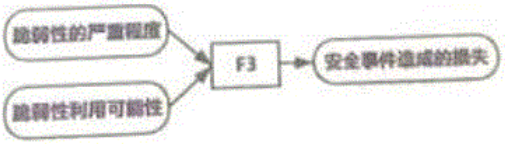
A.



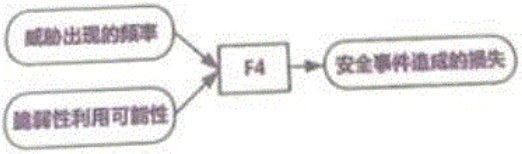
B.



C.



D.



A

212. 某软件公司准备提高其开发软件的安全性，在公司内部发起了有关软件开发生命周期的讨论，在下面的发言观点中，正确的是（）

A.软件安全开发生命周期较长，而其中最重要的是要在软件的编码...好安全措施，就可以解决 90%以上的安全问题。

B.应当尽早在软件开发的需求和设计阶段增加一定的安全措施，这样可以比在软件发布以后进行漏洞修复所花的代价少得多。

C.和传统的软件开发阶段相比，微软提出的安全开发生命周期（securitydevetqpmefrtliocyclnsdl)的最大特点是增加了一个专门的安全编码阶段。

D.软件的安全测试也很重要，考试到程序员的专业性，如果该开发人员已经对软件进行了安全性测试，就没有必要再组织第三方进行安全性测试。

B

213. 某网站在设计对经过了威胁建模和攻击面分析，在开发时要求程序员编写安全的代码，但是在部署时由于管理员将备份存放在 WED 目录下导致了攻击者可直接下载备份，为了

发现系统中是否存在其他类拟问题，一下那种测试方式是最佳的测试方法。

A.模糊测试

B.源代码测试

C.渗透测试

D.软件功能测试

C

214. 下面哪项属于软件开发安全方面的问题（）

A.软件部署时所需选用服务性能不高，导致软件执行效率低。

B.应用软件来考虑多线程技术，在对用户服务时按序排队提供服务

C.应用软件存在 sol 注入漏洞，若被黑客利用能窃取数据库所用数据

D.软件受许可证（license）限制，不能在多台电脑上安装。

C

215. 为增强 Web 应用程序的安全性，某软件开发经理决定加强 Web 软件安全开发培训，下面哪项内容要在他的考虑范围内（）

A.关于网站身份签别技术方面安全知识的培训

B.针对 OpenSSL 心脏出血漏洞方面安全知识的培训

C.针对 SQL 注入漏洞的安全编程培训

D.关于 ARM 系统漏洞挖掘方面安全知识的培训

C

216. 以下关于 https 协议 http 协议相比的优势说明，那个是正确的：

A.Https 协议对传输的数据进行加密，可以避免嗅探等攻击行为

B.Https 使用的端口 http 不同，让攻击者不容易找到端口，具有较高的安全性

C.Https 协议是 http 协议的补充，不能独立运行，因此需要更高的系统性能

D.Https 协议使用了挑战机制，在会话过程中不传输用户名和密码，因此具有较高的

A

217.风险要素识别是风险评估实施过程中的一个重要步骤，小李将风险要素识别的主要过程使用图形来表示，如下图所示，请为图中空白框处选择一个最合适的选项（）。

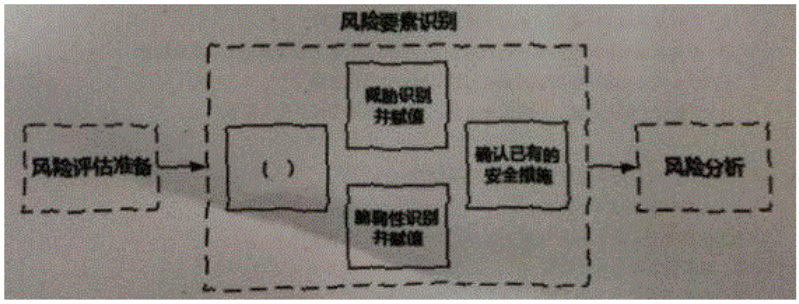
A.明确组织管理机构

B.制定安全措施实施计划

C. 资产识别并赋值

D. 风险识别并赋值

C



218. 规范的实施流程和文档管理，是信息安全风险评估结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。

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

D P74 页

219. 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（）。

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缺失量

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和直接进行，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

B

220.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（）。

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收，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，明确信息安全风险管理作用，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

221.小李去参加单位组织的信息安全管理体系（Information Securlty Management System. ISMS）的理解画了一下一张图，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（）。

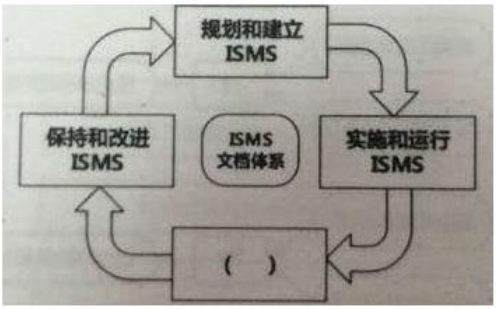
A.监控和反馈 ISMS

B.批准和监督 ISMS

C.监视和评审 ISMS

D.沟通和咨询 ISMS

C 课本 86 页原文内容



222.在某个信息系统实施案例中，A 单位（甲方）允许 B 公司（乙方）在甲方的测试天

南地北中开发和部署业务系统，同时为防范风险，A 单位在和 B 公司签订合同中，制定有关条款，明确了如果由于B 公司操作原因引起的设备损坏，则B 公司需按价赔偿。可以看出，该赔偿条款应用了风险管理中（）的风险处置措施。

A.降低风险

B.规避风险

C.转移风险

D.拒绝风险

C 授课老师所讲，PPT 上有对应内容

223.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，（）规定了等级保护定级阶段的依据、对象、流程、方法及等级变更等内容。

A.GB / T 20271-2006《信息系统通用安全技术要求》

B.GB / T 22240-2008《信息系统安全保护等级定级指南》

C.GB / T 25070-2010《信息系统等级保护安全设计技术要求》

D.GB / T 20269-2006《信息系统安全管理要求》

B

224.GB / T 18336《信息技术安全性评估准则》是测评标准类中的重要标准，该标准定义了评估对象（Targetof Evaluation，TOE）、保护轮廓（Protection Profile，PP）和安全目标（Security Target，ST）等术语。关于安全目标(ST)，下面选项中描述错误的是()。

A.ST 阐述了安全要求，具体说明了一个既定被评估产品或评估对象的安全功能

B.ST 包括该 TOE 的安全要求和用于满足安全要求的特定安全功能和保证措施

C.ST 对于产品和系统来讲，相当于要求了其安全实现方案

D.ST 从用户角度描述，代表了用户想要的东西，而不是厂商声称提供的东西

D

225.关于密钥管理，下列说法错误的是：

A.科克霍夫原则指出算法的安全性不应基于算法的保密，而应基于密钥的安全性

B.保密通信过程中，通信方使用之前用过的会话密钥建立会话，不影响通信安全

C.密钥管理需要考虑密钥产生、存储、备份、分配、更新、撤销等生命周期过程的每一个环节

D.在网络通信中，通信双方可利用 Diffie-Hellman 协议协商出会话密钥

B

226.某移动智能终端支持通过指纹识别解锁系统的功能，与传统的基于口令的鉴别技术相比，关于此种鉴别技术说法不正确的是：

A.所选择的特征（指纹）便于收集、测量和比较

B.每个人所拥有的指纹都是独一无二的

C.指纹信息是每个人独有的，指纹识别系统不存在安全威胁问题

D.此类系统一般由用户指纹信息采集和指纹信息识别两部分组成

c

227.以下 Windows 系统的账号存储管理机制 SAM（Security Accoumts Manager）的说法哪个是正确的：

A.存储在注册表中的账号数据是管理员组用户都可以访问，具有较高的安全性

B.存储在注册表中的账号数据只有 administrator 账户才有权访问，具有较高的安全性

C.存储在注册表中的账号数据任何用户都可以直接访问，灵活方便

D.存储在注册表中的账号数据只有 System 账号才能访问，具有较高的安全性

D

228.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：

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

B

229.以下关于 SMTP 和 POP3 协议的说法哪个是错误的：

64

A.SMTP 和 POP3 协议是一种基于 ASCII 编码的请求/响应模式的协议

B.SMTP 和 POP3 协议明文传输数据，因此存在数据泄漏的可能

C.SMTP 和 POP3 协议缺乏严格的用户认证，因此导致了垃圾邮件问题

D.SMTP 和 POP3 协议由于协议简单，易用性更高，更容易实现远程管理邮件

C

230.某公司的对外公开网站主页经常被黑客攻击后修改主页内容，该公司应当购买并部署下面哪个设备（）？

A.安全路由器

B.网络审计系统

C.网页防篡改系统

D.虚拟专用网（Virtual Private Network，VPN）系统

C

231.安全多用途互联网邮件扩展（SecureMultipurpose Internet Mail Extension，S/MIME）是指一种保障邮件安全的技术，下面描述错误的是（）。

A.S/MIME 采用了非对称密码学机制

B.S/MIME 支持数字证书

C.S/MIME 采用了邮件防火墙技术

D.S/MIME 支持用户身份认证和邮件加密

C

232.关于恶意代码，以下说法错误的是：

A.从传播范围来看，恶意代码呈现多平台传播的特征。

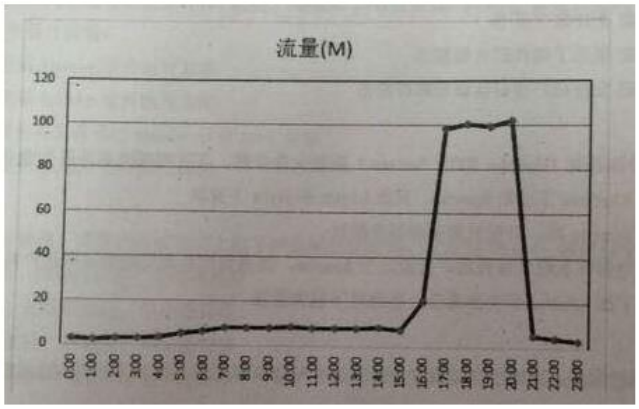
B.按照运行平台，恶意代码可以分为网络传播型病毒、文件传播型病毒。

C.不感染的依附性恶意代码无法单独执行

D.为了对目标系统实施攻击和破坏活动，传播途径是恶意代码赖以生存和繁殖的基本条件

B

233.下图是某单位对其主网站的一天访问流量监测图，如果说该网站在当天 17：00 到 20：00 间受到了攻击，则从图中数据分析，这种攻击类型最可能属于下面什么攻击（）。



A.跨站脚本（Cross Site Scripting，XSS）攻击

B.TCP 会话劫持（TCP Hijack）攻击

C.IP 欺骗攻击

D.拒绝服务（Denial of Service，DoS）攻击

D

234.当前，应用软件安全已经日益引起人们的重视，每年新发现的应用软件漏洞已经占新发现漏洞总数一半以上。下列选项中，哪个与应用软件漏洞成因无关：

A.传统的软件开发工程未能充分考虑安全因素

B.开发人员对信息安全知识掌握不足

C.相比操作系统而言，应用软件编码所采用的高级语言更容易出现漏洞

D.应用软件的功能越来越多，软件越来越复杂，更容易出现漏洞

C

235.下面哪个模型和软件安全开发无关（）？

A.微软提出的“安全开发生命周期（Security Development Lifecycle,SDL）”

B.Gray McGraw 等提出的“使安全成为软件开发必须的部分（Building Security IN，BSI ） ”

C.OWASP 维护的“ 软件保证成熟度模型（ Software Assurance Maturity Mode,SAMM）”

D.美国提出的“信息安全保障技术框架（Information Assurance Technical Framework，IATF）”

D

236.某网站为了开发的便利，SA 连接数据库，由于网站脚本中被发现存在 SOL 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：

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

B

237.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：

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

D

238.以下关于模糊测试过程的说法正确的是：

A.模糊测试的效果与覆盖能力，与输入样本选择不相关

B.为保障安全测试的效果和自动化过程，关键是将发现的异常进行现场保护记录，系统可能无法恢复异常状态进行后续的测试

C.通过异常样本重现异常，人工分析异常原因，判断是否为潜在的安全漏洞，如果是安全漏洞，就需要进一步分析其危害性、影响范围和修复建议

D.对于可能产生的大量异常报告，需要人工全部分析异常报告__

C

239. 某公司开发了一个游戏网站，但是由于网站软件存在问题，结果在软件上线后被黑客攻击，其数据库中的网游用户真实身份数据被黑客看到。关于此案例，可以描述正确的是（）

A 该网站软件出现了保密性方面安全问题

B 该网站软件出现了完整性方面安全问题

C 该网站软件出现了可用性方面安全问题

D 该网站软件出现了不可否认性方面安全问题

A

240. 我国信息安全保障工作先后经历了启动、逐步展开和积极推进，以及深化落实三个阶段，以下关于我国信息安全保障各阶段说法不正确的是：

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

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

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

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

B 积极防御，综合防范

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

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

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

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

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

B

242. 以下关于安全套接层协议（Secure Sockets Layer,SSL）说法错误的是：

A. SSL 协议位于 TCPAP 协议层和应用协议之间

B. SSL 协议广泛应用于 web 浏览器与服务器之间的身份认证和加密数据传输

C. SSL 是一种可靠的端到端的安全服务协议

D. SSL 是设计用来保护操作系统的

D

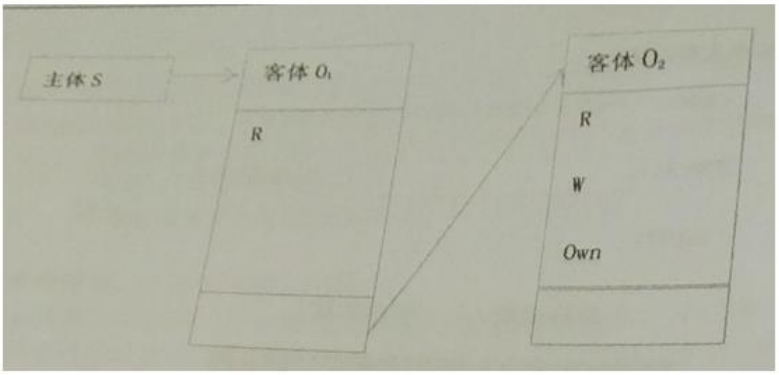
243. 如图所示，主体 S 对客体 01 有读（R）权限，对客体 02 有读（R）、写（）权限。该图所示的访问控制实现方法是：

A. 访问控制表（ACL）

B. 访问控制矩阵

C. 能力表（CL）

D. 前缀表（Profiles）



C

244. 关于 Kerberos 认证协议，以下说法错误的是：

A. 只要用户拿到了认证服务器（AS）发送的票据许可票据（TGT）并且该 TGT 没有过期，就可以使用该 TGT 通过票据授权服务器（TGS）完成到任一个服务器的认证而不必重新输入密码

B. 认证服务器(AS)和票据授权服务器(TGS)是集中式管理，容易形成瓶颈，系统的性能和安全也严重依赖于 AS 和 TGS 的性能和安全

C. 该协议通过用户获得票据许可票据、用户获得服务许可票据、用户获得服务三个阶段，仅支持服务器对用户的单向认证

D. 该协议是一种基于对称密码算法的网络认证协议，随用户数量增加，密钥管理较复杂

C

245.以下哪个选项不是防火墙技术？

A.IP 地址欺骗防护

B.NAT

C.访问控制

D.SQL 注入攻击防护

D

246.Linux/Unix 关键的日志文件设置的权限应该为

A.-rw-r--r-

B.-rw----

C.-rw-rw-rw-

D.-r-----

A 不太确定

247.张主任的计算机使用 Windows7 操作系统，他常登陆的用户名为 zhang,张主任给他个人文件夹设置了权限为只有 zhang 这个用户有权访问这个目录，管理员在某次维护中无意将 zhang 这个用户删除了，随后又重新建了一个用户名为 zhang，张主任使用 zhang 这个用户登录系统后，发现无法访问他原来的个人文件夹，原因是：

A.任何一个新建用户都需要经过授权才能访问系统中的文件

B.windows7 不认为新建立的用户 zhang 与原来的用户 zhang 是同一个用户，因此无法访问

C.用户被删除后，该用户创建的文件夹也会自动删除，新建用户找不到原来用户的文件夹，因此无法访问

D.新建的用户 zhang 会继承原来用户的权限，之所以无法访问是因为文件夹经过了加密

B

248.口令破解是针对系统进行攻击的常用方法，Windows 系统安全策略应对口令破解的策略主要是账户策略中的账户锁定策略和密码策略，关于两个策略说明错误的是

A.密码策略的主要作用是通过策略避免用户生成弱口令及对用户的口令使用进行管控

B.密码策略对系统中所有的用户都有效

C.账户锁定策略的主要作用是应对口令暴力破解攻击，能有效的保护所有系统用户应对口令暴力破解攻击

D.账户锁定策略只适用于普通用户，无法保护管理员 administrator 账户应对口令暴力破解攻击

D

249.以下关于账户密码策略中各项策略的作用说明，哪个是错误的：

A.“密码必须符合复杂性要求”是用于避免用户产生诸如 1234、1111 这样的弱口令

B.“密码长度最小值”是强制用户使用一定长度以上的密码

C.“强制密码历史”是强制用户不能再使用曾经使用过的任何密码

D.“密码最长存留期”是为了避免用户使用密码时间过长而不更户

C

强制密码历史:

重新使用旧密码之前，该安全设置确定与某个用户帐户相关的唯一新密码的数量。该值必须为 0 到 24 之间的一个数值。

该策略通过确保旧密码不能继续使用，从而使管理员能够增强安全性。

250.以下 SQL 语句建立的数据库对象是：

A.表

B.视图

C.存储过程

D.触发器

CREATE VIEW PatientsForDoctors AS

SWLWCT Patient

FROM Patient*

WHERE doctorID=123

B

251.某政府机构委托开发商开发了一个 OA 系统,其中有一个公文分发,公文通知等为 WORD 文档，厂商在进行系统设计时使用了 FTP 来对公文进行分发，以下说法不正确的是

A FTP 协议明文传输数据，包括用户名和密码，攻击者可能通过会话过程嗅探获得 FTP 密码，从而威胁 OA 系统

B FTP 协议需要进行验证才能访问在，攻击者可以利用 FTP 进行口令的暴力破解

C FTP 协议已经是不太使用的协议，可能与新版本的浏览器存在 兼容性问题

D FTP 应用需要安装服务器端软件，软件存在漏洞可能会影响到 OA 系统的安全

C

252.某公司在互联网区域新建了一个 WEB 网站，为了保护该网站主页安全性，尤其是不能让攻击者修改主页内容，该公司应当购买并部署下面哪个设备（）

A 负载均衡设备

B 网页防篡改系统

C 网络防病毒系统

D 网络审计系统

B

253.小陈在某电器城购买了一台冰箱，并留下了个人姓名、电话在和电子邮件地址等信，第二天他收到了一封来自电器城提示他中奖的邮件上，查看该后他按照提示操作，纳中奖税款后并没有得到中奖奖金，再打电话询问电器城才得知电器城并没有开的活动，根据上面的描述，由此可以推断的是（）

A.小陈在电器城登记个人信息时，应当使用加密手段

B.小陈遭受了钓鱼攻击，钱被骗走了

C.小陈的计算机中了木马，被远程控制

D.小陈购买的凌波微步是智能凌波微步 ，能够自己上网

B

254.小王在某 WEB 软件公司工作，她在工作中主要负责对互联网信息服务（ Internet information services,iis)软件进行安全配置，这是属于（） 方面的安全工作

A.WEB 服务支撑软件

B.WEB 应用程序

C.WEB 浏览器

D.通信协议

A

255.在 2014 年巴西世界杯举行期间,，一些黑客组织攻击了世界杯赞助商及政府网站，

制了大量网络流量，阻塞正常用户访问网站。这种攻击类型属于下面什么攻击（）

A.跨站脚本（ cross site scripting,XSS)攻击

B.TCP 会话劫持（ TCP HIJACK)攻击

C.ip 欺骗攻击

D.拒绝服务（denialservice.dos）攻击

D

256.以下可能存在 sql 注入攻击的部分是

A.get 请求参数

B.post 请求参数

C.cookie 值

D.以上均有可能

D

257.关于软件安全的问题，下面描述错误的是（）

A.软件的安全问题可能造成软件运行不稳定，得不到正确结果甚至崩溃

B.软件问题安全问题应依赖于软件开发的设、编程、测试以及部署等各个阶段措施来解决

C.软件的安全问题可能被攻击者利用后影响人身体健康安全

D.软件的安全问题是由程序开发者遗留的，和软件的部署运行环境无关

D

258.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，在厦下面做法中，对于解决问题没有直接帮助的是（）

A.要求开发人员采用敏捷开发模型进行开发

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

A

259.关于源代码审核，描述错误的是（）

A.源代码审核有利于发现软件编码中存在的安全问题

B.源代码审核工程遵循 PDCA 模型

C.源代码审核方式包括人工审核工具审核

D.源代码审核工具包括商业工具和开源工具

不确定

B

260.关于风脸要素识别阶段工作内容叙述错误的悬：

A．资产识别是指对需要保护的资产和系统等进行识别和分类

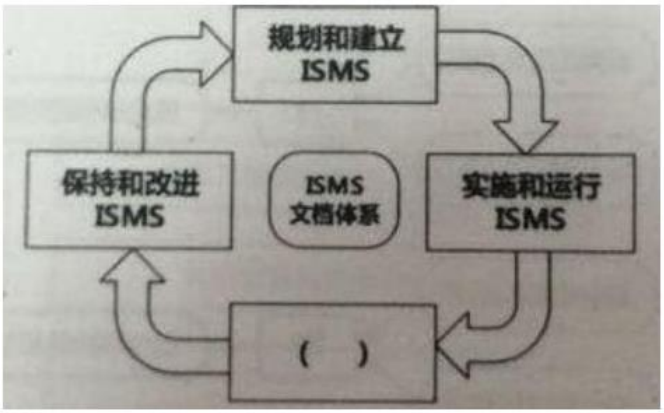
B．威胁识别是指识别与每项资产相关的可能威胁和漏洞及其发生的可能性

C．脆弱性识别以资产为核心，针对每一项需要保护的资产。识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估

D．确认已有的安全措施仅属于技术层面的工作，牵涉到具体方面包括：物理平台、系统平台、网络平台和应用平台

D

261. 小李去参加单位组织的信息安全后，他把自己对信息安全管理体系（Information Securlty Management System. ISMS）的理解画了以下一张图，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（）。



A.监控和反馈 ISMS

B.批准和监督 ISMS

C.监视和评审 ISMS

D.沟通和咨询 ISMS

C

262. 信息安全管理体系（information Securlty Management System. 简称 ISMS）要求

建立过程体系，该过程体系是在如下（）基础上构建的。

A.IATF（Information Assurance Technical Framework）

B.P2DR(Policy，Protection，Detection，Response)

C.PDCERF(Preparation，Detection，Containment，Eradication，Recovery，Follow-up)

D.PDCA（Plan，Do，Check，Act）

D

263.对系统工程（Systems Engineering，SE)的理解，以下错误的是：

A.系统工程偏重于对工程的组织与经营管理进行研究

B.系统工程不属于技术实现，而是一种方法论

C.系统工程不是一种对所有系统都具有普遍意义的科学方法

D.系统工程是组织管理系统规划、研究、制造、试验、使用的科学方法

A

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

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 Areas，PA）具备了“定义标准过程”、“执行已定义的过程”两个公共特征，则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 Areas，PA）包含4个基本实施（Base Practices，BP)，执行此PA时执行了3个BP，则此过程区域的能力成熟度级别为0

D.组织在不同的过程区域的能力成熟度可能处于不同的级别上

B

265.标准是标准化活动的成果，是为了在一定范围内获得最佳秩序，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，关于标准和标准化，以下选项中理解错误的是（）。

A.标准化是一项活动，标准化工作的主要任务是定标准、组织实施以及对标准的实施进行监督，主要作用是为了预期的目的而改进产品、过程或服务的实用性，防止壁垒，促进合作

B.标准化的对象不应是孤立的一件事或一个事物，而是共同的、可重复的事物，标准化

的工作同时也具有动态性，即应随着科学的发展和社会的进步而不断修订标准

C.标准在国际贸易中有着重要作用，一方面，标准能打破技术壁垒，促进国际间的经贸发展和科学、技术、文化交流和合作；另一方面，标准也能成为新的技术壁垒，起到限制他国产品出口、保护本国产业的目的

D.标准有着不同的分类，我国将现有标准分为强制性标准、推荐性标准和事实性标准三类，国家标准管理机构对着三类标准通过采取不同字头的方式分别编号后公开发布

D

指导性标准

266. 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。

A.GB／T 22239-2008《信息系统等级保护安全设计技术要求》

B.GB／T 22240-2008《信息系统安全保护等级定级指南》

C.GB／T 25070-2010《信息系统等级保护安全设计技术要求》

D.GB／T 28449-2012《信息系统安全等级保护测评过程指南》

B