信息安全专业人员知识测试试题（二）

1. 我国信息安全保障工作先后经历启动、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 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《关于加强信息安全保障工作的意见》（中办发 27 号文），明确了“积极防御、综合防范“的国家信息安全保障方针
   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。
   解释：2006 年进入到深化落实阶段。

2. 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纪录和表单数据
   解释：A 为正确答案。

3. 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，以下关于安全保障建设主要工作内容说法不正确的是：
   A. 建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
   解释：实现自主创新在过去的的保障中为自主可控。

4. 某银行信息系统为了满足业务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
   解释：无法消除或降低该银行信息系统面临的所有安全风险。

5. 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的产品的安全性做出的独立评价，增强用户对已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，提出游针对性的安全防护策略和整改措施
   解释：测评包括产品测评、风险评估、保障测评和等级保护测评。

6. 美国的关键信息基础设施（Critical Information Infrastructure,CII）包括商用核设施、政策设施、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。
   解释：从题目中不能反映 C 的结论。

7. 在设计信息系统安全保障方案时，以下哪个做法是错误的：
   A.要充分切合信息安全需求并且实际可行
   B.要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量控制成本
   C.要充分采取新技术，使用过程中不断完善成熟，精益求精，实现技术投入保值要求
   D.要充分考虑用户管理和文化的可接受性，减少系统方案障碍

解释：设计信息系统安全保障方案应采用合适的技术。

8. 分组密码算法是一类十分重要的密码算法，下面描述中，错误的是（）
A.分组密码算法要求输入明文按组分成固定长度的块 B.分组密码的算法每次计算得到固定长度的密文输出块
C.分组密码算法也称作序列密码算法 D.常见的 DES、IDEA 算法都属于分组密码算法
解释：分组密码算法和序列算法是两种算法。

9. 密码学是网络安全的基础，但网络安全不能单纯依靠安全的密码算法、密码协议也是网络安全的一个重要组成部分。下面描述中，错误的是（）
A.在实际应用中，密码协议应按照灵活性好、可扩展性高的方式制定，不要限制和框住的执行步骤，有些复杂的步骤可以不明确处理方式。
B.密码协议定义了两方或多方之间为完成某项任务而指定的一系列步骤，协议中的每个参与方都必须了解协议，且按步骤执行。
C.根据密码协议应用目的的不同，参与该协议的双方可能是朋友和完全信息的人，也可能是敌人和互相完全不信任的人。
D.密码协议(Crypto graphic protocol) ,有时也称安全协议(security protocol), 是使用密码学完成某项特定的任务并满足安全需求的协议，其末的是提供安全服务。
解释：密码协议应限制和框住的执行步骤，有些复杂的步骤必须要明确处理方式。

10. 部署互联网协议安全虚拟专用网（Internet protocol Security Virtual Private Network,IPsec VPN）时，以下说法正确的是：
A. 配置 MD5 安全算法可以提供可靠的数据加密
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
解释：A 错误，MD5 提供完整性；B 错误，AES 提供的保密性；D 错误，AH 协议提供完整性、验证及抗重放攻击。

11. 虚拟专用网络（VPN）通常是指在公共网路中利用隧道技术，建立一个临时的，安全的网络。这里的**字母 P** 的正确解释是（）
A.Special-purpose. 特定、专用用途的 C.Private 私有的、专有的
B.Proprietary 专有的、专卖的 D.Specific 特种的、具体的
解释：C 为正确答案。

12. 以下 Windows 系统的账号存储管理机制 SAM（Security Accounts 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 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
解释：D 为正确答案。

13. 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 C.网页防篡改系统
B.网络审计系统 D.虚拟专用网（Virtual Private Network，VPN）系统
解释：网页防篡改系统用来防范 WEB 篡改。

14. 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，传播途径是恶意代码赖以生存和繁殖的基本条件
解释：按照运行平台，恶意代码可以分为 Windows 平台、Linux 平台、工业控制系统等。

15. 某单位对其主网站的一天访问流量监测图，图显示该网站在当天 **17：00 到 20：00** 间受到了攻击，则从数据分析，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 C.IP 欺骗攻击
B.TCP 会话劫持（TCP Hijack）攻击 D.拒绝服务（Denial of Service，DoS）攻击
解释：答案为 D。

16. 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
解释：无论高级和低级语言都存在漏洞。

17. 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.“信息安全保障技术框架（Information Assurance Technical Framework，IATF）”
解释：D 与软件安全开发无关，ABC 均是软件安全开发模型。

18. 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
解释：A 错，模糊测试是模拟异常输入；B 错，入口与边界点是测试对象；C 模糊测试记录和检测异常运行情况。

19. 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
解释：C 为模糊测试的涵义解释。

20. 关于 WI-FI 联盟提出的安全协议 WPA 和 WPA2 的区别。下面描述正确的是（）
A.WPA 是有线局域安全协议，而 WPA2 是无线局域网协议
B.WPA 是适用于中国的无线局域安全协议，WPA2 是使用于全世界的无线局域网协议
C.WPA 没有使用密码算法对接入进行认证，而 WPA2 使用了密码算法对接入进行认证
D.WPA 是依照 802.11i 标准草案制定的，而 WPA2 是按照 802.11i 正式标准制定的
解释：答案为 D。

21. 防火墙是网络信息系统建设中常常采用的一类产品，它在内外网隔离方面的作用是
A.既能物理隔离，又能逻辑隔离
B.能物理隔离，但不能逻辑隔离
C.不能物理隔离，但是能逻辑隔离
D.不能物理隔离，也不能逻辑隔离
解释：答案为 C。

22. 异常入侵检测是入侵检测系统常用的一种技术，它是识别系统或用户的非正常行为或者对于计算机资源的非正常使用，从而检测出入侵行为。下面说法错误的是
A.在异常入侵检测中，观察的不是已知的入侵行为，而是系统运行过程中的异常现象
B.实施**异常入侵检测**，是将当前获取行为数据和已知入侵攻击行为特征相比较，若匹配则认为有攻击发生
C.异常入侵检测可以通过获得的网络运行状态数据，判断其中是否含有攻击的企图，并通过多种手段向管理员报警
D.异常入侵检测不但可以发现从外部的攻击，也可以发现内部的恶意行为
解释：实施误用入侵检测（或特征检测），是将当前获取行为数据和已知入侵攻击行为特征相比较，若匹配则认为有攻击发生。

23. S 公司在全国有 20 个分支机构，总部由 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 5 公司选出设计最合理的一个:
A.总部使用服务器、用户终端统一使用 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。
解释：答案为 C，考核的是 IP 地址规划的体系化。

24. 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
解释：答案为 C。

25. 口令破解是针对系统进行攻击的常用方法，windows 系统安全策略中应对口令破解的策略主要是帐户策略中的帐户锁定策略和密码策略，关于这两个策略说明错误的是
A.密码策略主要作用是通过策略避免拥护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，能有效地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
解释：.账户锁定策略也适用于 administrator 账户。

26. windows 文件系统权限管理使用访问控制列表（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适用的是 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，为了使用上的便利,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的
D.由于 ACL 具有很好灵活性，在实际使用中可以为每一个文件设定独立拥护的权限
解释：Windows 的 ACL 机制中，文件和文件夹的权限是客体关联的，即文件夹和文件的访问权限信息是写在客体文件和文件夹属性数据库中。

27. 由于发生了一起针对服务器的口令暴力破解攻击，管理员决定对设置帐户锁定策略以对抗口令暴力破解。他设置了以下账户锁定策略如下：
- ✓ 账户锁定阀值 3 次无效登陆；
- ✓ 复位账户锁定计数器 5 分钟；
- ✓ 账户锁定时间 10 分钟；

以下关于以上策略设置后的说法哪个是正确的
A.设置账户锁定策略后，攻击者无法再进行口令暴力破解，所有输错的密码的拥护就会被锁住
B.如果正常用户部小心输错了 3 次密码，那么该账户就会被锁定 10 分钟，10 分钟内即使输入正确的密码，也无法登录系统
C.如果正常用户不小心连续输入错误密码 3 次，那么该拥护帐号被锁定 5 分钟，5 分钟内即使交了正确的密码，也无法登录系统
D.攻击者在进行口令破解时，只要连续输错 3 次密码，该账户就被锁定 10 分钟，而正常拥护登陆不受影响
解释：答案为 B，全部解释为 5 分钟计数器时间内错误 3 次则锁定 10 分钟。

28. 加密文件系统（Encrypting File System, EFS）是 Windows 操作系统的一个组件，以下说法错误的是（）
A.EFS 采用加密算法实现透明的文件加密和解密，任何不拥有合适密钥的个人或者程序都不能解密数据
B.EFS 以公钥加密为基础，并利用了 widows 系统中的 CryptoAPI 体系结构
C.EFS 加密系统适用于 NTFS 文件系统合 FAT32 文件系统（Windows 环境下）
D.EFS 加密过程对用户透明，EFS 加密的用户验证过程是在登陆 windows 时进行的
解释：答案为 C，FAT32 不支持 EFS 加密。

29. 关于数据库恢复技术，下列说法不正确的是：
A.数据库恢复技术的实现主要依靠各种数据的冗余和恢复机制技术来解决，当数据库中数据被破坏时，可以利用冗余数据来进行修复
B.数据库管理员定期地将整个数据库或部分数据库文件备份到磁带或另一个磁盘上保存起来，是数据库恢复中采用的基本技术
C.日志文件在数据库恢复中起着非常重要的作用，可以用来进行事务故障恢复和系统故障恢复，并协助后备副本进行介质故障恢复
D.计算机系统发生故障导致数据未存储到固定存储器上，利用日志文件中故障发生前数据的循环，将数据库恢复到故障发生前的完整状态，这一对事务的操作称为提交
解释：利用日志文件中故障发生前数据的循环，将数据库恢复到故障发生前完整状态，这一对事务的操作称为回滚。

30. 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.粒度最小的策略，将数据库中数据项进行划分，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
解释：数据库安全策略应为最小共享。

31. 数据在进行传输前，需要由协议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
解释：答案为 B。

32. 以下关于 SMTP 和 POP3 协议的说法哪个是错误的
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 协议铭文传输数据，因此存在数据泄露的可能
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
解释：基于 HTTP 协议或 C/S 客户端实现邮件的远程管理。

33. 安全多用途互联网邮件扩展(Secure Multipurpose 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
解释：S/MIME 是邮件安全协议，不是防火墙技术。

34. 应用安全，一般是指保障应用程序使用过程和结果的安全。以下内容中不属于应用安全防护考虑的是（）
A.身份鉴别，应用系统应对登陆的用户进行身份鉴别，只有通过验证的用户才能访问应用系统资源
B.安全标记，在应用系统层面对主体和客体进行标记，主体不能随意更改权限，增加访问
C.剩余信息保护，应用系统应加强硬盘、内存或缓冲区中剩余信息的保护，防止存储在硬盘、内存或缓冲区的信息被非授权的访问
D.机房与设施安全，保证应用系统处于有一个安全的环境条件，包括机房环境、机房安全等级、机房的建造和机房的装修等
解释：机房与设施安全属于物理安全，不属于应用安全。

35. Ａｐａｃｈｅ Ｈｔｔｐ Ｓｅｒｖｅｒ（简称 Ａｐａｃｈｅ）是一个开放源码的ＷＥＢ服务运行平台，在使用过程中，该软件默认会将自己的软件名和版本号发送给客户端。从安全角度出发，为隐藏这些信息，应当采取以下那种措施（）
A.安装后，修改访问控制配置文件
B.安装后，修改配置文件 Httpd．Conf 中的有关参数
C.安装后，删除Ａｐａｃｈｅ Ｈｔｔｐ Ｓｅｒｖｅｒ源码
D.从正确的官方网站下载Ａｐａｃｈｅ Ｈｔｔｐ Ｓｅｒｖｅｒ，并安装使用
解释：答案为 B。

36. 下面信息安全漏洞理解错误的是：
A.讨论漏洞应该从生命周期的角度出发，信息产品和信息系统在需求、设计、实现、配置、维护和使用等阶段中均有可能产生漏洞
B.信息安全漏洞是由于信息产品和信息系统在需求、设计、开发、部署或维护阶段，由于设计、开发等相关人员无意中产生的缺陷所造成的
C.信息安全漏洞如果被恶意攻击者成功利用，可能会给信息产品和信息系统带来安全损害，甚至带来大的经济损失
D.由于人类思维能力、计算机计算能力的局限性等因素，所以在信息产品和信息系统中产生新的漏洞是不可避免的
解释：安全漏洞可以有意产生，也会无意产生。

37. 下面对“零日（ｚｅｒｏ－ｄａｙ）漏洞”的理解中，正确的是（）
A.指一个特定的漏洞，该漏洞每年 1 月 1 日零点发作，可以被攻击者用来远程攻击，获取主机权限
B.指一个特定的漏洞，特指在２０１０年被发现出来的一种漏洞，该漏洞被“震网”病毒所利用，用来攻击伊朗布什尔核电站基础设施
C.指一类漏洞，即特别好被利用，一旦成功利用该类漏洞，可以在 1 天内文完成攻击，且成功达到攻击目标
D.指一类漏洞，即刚被发现后立即被恶意利用的安全漏洞，一般来说，那些已经被小部分人发现，但是还未公开、还不存在安全补丁的漏洞都是零日漏洞
解释：D 是零日漏洞的解释。

38. 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？我是科技处的李强，我的邮箱密码忘记了，现在打不开邮件，我着急收割邮件，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者的要求，随后，李强发现邮箱系统登陆异常，请问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小张没按照操作流程工作
D.事件属于邮件系统故障，是偶然事件，应向单位领导申请邮件服务软件
解释：该题目考点为信息安全措施的操作安全，要求一切操作均有流程。

39. 某网站管理员小邓在流量监测中发现近期网站的入站ＩＣＭＰ流量上升了２５０％，尽管网站没有发现任何的性能下降或其他问题。但为了安全起见，他仍然向主管领导提出了应对策略，作为主管负责人，请选择有效的针对此问题的应对措施：
A.在防火墙上设置策略，阻止所有的ＩＣＭＰ流量进入　　B.删除服务器上的ｐｉｎｇ．ｅｘｅ程序
C.增加带宽以应对可能的拒绝服务攻击　　D.增加网站服务器以应对即将来临的拒绝服务攻击
解释：A 是应对措施。

40. 下面四款安全测试软件中，主要用于 WEB 安全扫描的是（）
A.CIsco Auditing Tools　　B.Acunetix Web Vulnerability Scanner　　C.NMAP　　D.ISS Database Scanner
解释：B 为 WEB 扫描工具。

41. 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设，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，并在使用前对数据进行校验
解释：SQL 注入与编码 SQL 语法应用和过滤有关，与开发语言不是必然关系。

42. 在软件保障成熟度模型（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和活动
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
解释：ＳＡＭＭ包括治理、构造、验证、部署。

43. 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，阶段较多，而其中最重要的是要在软件的编码阶段做好安全措施，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就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的多。
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的最大特点是增加了一个抓们的安全编码阶段
D.软件的安全测试也很重要，考虑到程序员的专业性，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
解释：正确答案为 B。

44. 下面有关软件安全问题的描述中，哪项是由于软件设计缺陷引起的（）
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
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
解释：答案为Ｃ。

45. 软件存在漏洞和缺陷是不可避免的，实践中常使用软件缺陷密度（Ｄｅｆｅｃｔｓ／ＫＬＯＣ）来衡量软件的安全性，假设某个软件共有２９．６万行源代码，总共被检测出１４５个缺陷，则可以计算出其软件缺陷密度值是
A.０．０００４９　　B.０．０４９　　C.０．４９　　D.４９
解释：千行代码缺陷率计算公式，145/(29.5*10)=0.49。

46. 某集团公司根据业务需求，在各地分支机构部属前置机，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种提取日志，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，通过设置前置机不记录日志
D.只允许特定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
解释：D 的特定ＩＰ地址从前置机提取降低了开放日志共享的攻击面。

47. 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，以下哪个不是需求考虑的攻击方式
A.攻击者利用软件存在的逻辑错误，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咨询，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ＩＤＣ人员，将某软件运行服务器的网线拔掉导致无法访问
解释：D 为社会工程学攻击。

48. 某网站为了开发的便利，使用 **SA** 链接数据库，由于网站脚本中被发现存在 SQL 注入漏洞，导致攻击者利用内置存储过程 XP.cmctstell 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
解释：SA 是数据库最大用户权限，违反了最小特权原则。

49. 微软提出了 STRIDE 模型，其中 Repudation（抵赖）的缩写，关于此项安全要求，下面描述**错误**的是（）
A.某用户在登陆系统并下载数据后，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
解释：STRIDE 代表 6 种威胁的简称，无严重程度之分。S-欺骗，T-篡改，R-抵赖，I-信息泄露，D-拒绝服务，E-权限提升（攻击）。

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

51. 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（）
A.信息安全管理体系（ISMS） B.信息安全等级保护 C.NIST SP800 D.ISO 270000 系统
解释：信息安全等级保护制度重点保障基础信息网络和重要信息系统的安全。

52. 小明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几本概念与认识，小明的主要观点包括：
（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，完成信息安全风险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
请问小明的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
解释：背景建立是根据政策、法律、标准、业务、系统、组织等现状来开展。

53. 降低风险（或减低风险）指通过对面的风险的资产采取保护措施的方式来降低风险，下面那个措施不属于降低风险的措施（）
A.减少威胁源，采用法律的手段制裁计算机的犯罪，发挥法律的威慑作用，从而有效遏制威胁源的动机
B.签订外包服务合同，将有计算难点，存在实现风险的任务通过签订外部合同的方式交予第三方公司完成，通过合同责任条款来应对风险

C.减低威胁能力，采取身份认证措施，从而抵制身份假冒这种威胁行为的能力
D.减少脆弱性，及时给系统打补丁，关闭无用的网络服务端口，从而减少系统的脆弱性，降低被利用的可能性
解释：B 属于转移风险。

54. 关于风险要素识别阶段工作内容叙述错误的是：
A.资产识别是指对需求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，针对每一项需求保护的资产，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
解释：安全措施既包括技术层面，也包括管理层面。

55. 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
解释：检查评估由上级管理部门组织发起；本级单位发起的为自评估。

56. 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，按照规范的风险评估实施流程，下面哪个文档应当是风险要素识别阶段的输出成果（）
A,《风险评估方案》 B.《需要保护的资产清单》 C.《风险计算报告》 D.《风险程度等级列表》
解释：风险要素包括资产、威胁、脆弱性、安全措施。

57. 在信息安全管理的实施过程中，管理者的作用于信息安全管理体系能否成功实施非常重要，但是一下选项中不属于管理者应有职责的是（）
A.制定并颁发信息安全方针，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、可事实
C.向组织传达满足信息安全的重要性，传达满足信息安全要求、达成信息安全目标、符合信息安全方针、履行法律责任和持续改进的重要性
D.建立健全信息安全制度，明确安全风险管理作用，**实施信息安全风险评估过程、确保信息安全风险评估技术选择合理、计算正确**
解释：D 不属于管理者的职责。

58. 信息安全管理体系（Information Security 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，下面描述的错误是
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形式进行
C.内部审核实施主体组织内部的 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**
D.组织的信息安全方针、信息安全目标和有关 ISMS 文件等，在内部审核中作为审核标准使用，但在管理评审总，这些文件时被审对象
解释：管理评审的实施主体由用户的管理者来进行选择。

59. 在风险管理中，残余风险是指实施了新的或增强的安全措施后还剩下的风险，关于残余风险，下面描述错误的是（）
A.风险处理措施确定以后，应编制详细的残余风险清单，并获得管理层对残余风险的书面批准，这也是风险管理中的一个重要过程
B.管理层确认接收残余风险，是对风险评估工作的一种肯定，表示管理层已经全面了解了组织所面临的风险，并理解在风险一旦变为现实后，组织能够且承担引发的后果
C.接收残余风险，则表明没有必要防范和加固所有的安全漏洞，也没有必要无限制的提高安全保护措施的强度，对安全保护措施的选择要考虑到成本和技术等因素的限制
D.如果残余风险没有降低到可接受的级别，则只能被动的选择接受风险，**即对风险不进行下一步的处理措施**，接受风险可能带来的结果。
解释：如果残余风险没有降低到可接受的级别，则会被动的选择接受残余风险，但需要对残余风险进行进一步的关注、监测和跟踪。

60. 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，减少业务风此案而建立的一个控制过程。
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，减少业务风此案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，减少信息系统风险建立的一个控制过程
解释：业务连续性计划（BCP）是解决关键业务不中断。

61. 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、格式化被感染而已程序的介质**等，请问，按照应急响应方法，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**
解释：消除或阻断攻击源等措施为根除阶段。

62. 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急突发/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过程、系统损失和社会影响三方面。
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）
解释：应急响应包括六个阶段，为准备、检测、遏制、根除、恢复、跟踪总结。

63. 对信息安全事件的分级参考下列三个要素：信息系统的重要程度、系统损失和社会影响，依据信息系统的重要程度对信息进行划分，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**
解释：我国标准中未定义关键信息系统。

64. 恢复时间目标（RTO）和恢复点目标（RPO）是信息系统灾难恢复中的重要概念，关于这两个值能否为零，正确的选项是（）
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，但 RPO 可以为 0
D.RTO 不可以为 0，RPO 也不可以为 0
解释：RTO 可以为 0，RPO 也可以为 0。

65. 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，一期目标为年内实现系统上线运营，二期目标为次年上半年完成运行系统风险的处理：招标文件经营管理层审批后发布，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.招标文件经营管理层审批，表明工程目标符合业务发展规划
解释：题目描述不符合信息安全工程的“同步规划、同步实施”的基本原则。

66. 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、实验、使用的科学方法
解释：系统工程是一种对所有系统都具有普遍意义的科学方法

67. 系统工程的模型之一霍尔三维结构模型由时间维、逻辑维和知识维组成。 有关此模型，错误的是：
A.霍尔三维机构体系形成地描述了系统工程研究的框架
B.时间维表示系统工程活动从开始到结束按照时间顺序排列的全过程
C.逻辑维的七个步骤与时间维的七个阶段严格对应，即时间维第一阶段应执行逻辑维第一步骤的活动，时间维第二阶段应执行逻辑维第二步骤的活动
D.知识维列举可能需要运用的工程、医学、建筑、商业、法律、管理、社会科学和艺术等各种知识和技能
解释：霍尔三维模型是一种系统思想，无法实现严格的对应。

68. 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为 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。
解释：A 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为 0 级

B 错误，每次质量结果难以相同。C 错误，SSE-CMM 定义了一个风险过程，包括四个部分，评估影响、评估威胁、评估脆弱性、评估安全风险。D 错误，SSE-CMM 强调的是关联性而非独立性。

69. 以下哪一项不是信息系统集成项目的特点：
A.信息系统集成项目要以满足客户和用户的需求为根本出发点。
B.系统集成就是选择最好的产品和技术，开发响应的软件和硬件，将其集成到信息系统的过程。
C.信息系统集成项目的指导方法是“总体规划、分步实施”。
D.信息系统集成包含技术，管理和商务等方面，是一项综合性的系统工程
解释：系统集成就是选择最适合的产品和技术。

70. 信息安全工程监理是信息系统工程监理的重要组成部分，信息安全工程监理适用的信息化工程中，以下选择最合适的是：
A.通用布缆系统工程 B.电子设备机房系统工程 C.计算机网络系统工程 D.以上都适用
解释：答案为 D。

71. 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
解释：C 为安全工程的同步规划、同步实施原则。

72. 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 是没有进过测试的
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
解释：A 答案中 BP 是基于工程实践总结的工程单元。B 答案中 BP 是经过测试和实践验证的。C 答案中一项 BP 适用于组织的生存周期是正确的。D 一项 BP 不能和其他 BP 重叠。

73. 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 Aractices ，PA）活动**而非所有 PA 的活动**
C.在工程实施时，GP 应该作为基本实施（ 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
解释：GP 适用于域维中所有 PA 活动。

74. 在使用系统安全工程-能力成熟度模型（SSE-CCM）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
解释：SSE-CMM 充分定义级包括三个特征，为“定义标准过程”、“执行已定义的过程”、“安全协调实施”。B 答案中只描述了两个公共特征。

75. 系统安全工程-能力成熟度模型(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**
解释：风险过程包括评估影响、评估威胁、评估脆弱性和评估安全风险。

76. .以下行为不属于违反**国家涉密**规定的行为：
A.将涉密计算机、涉密存储设备接入互联网及其他公共信息网络 C.在私人交往中涉及国家秘密
B.通过普通邮政等无保密及措施的渠道传递国家秘密载体 D.以不正当手段获取商业秘密
解释：D 为商业秘密，不属于涉密规定的行为。

77. 具有行政法律责任强制的安全管理规定和安全制度包括

1）安全事件（包括安全事故）报告制度
2）安全等级保护制度
3）信息系统安全监控
4）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
解释：1\2\4 均为管理规定和安全制度。

78. 信息系统建设完成后，（ ）的信息系统的而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
解释：答案为 B，三级以上默认包括本级。

79. 为了保障网络安全，维护网络安全空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，加强在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了一部法律草案，并与 7 月 6 日起在网上全文公布，向社会公开征求意见，这部法律草案是（）
A.《中华人民共和国保守国家秘密法（草案）》
B.《中华人民共和国网络安全法（草案）》
C.《中华人民共和国国家安全法（草案）》
D.《中华人民共和国互联网安全法（草案）》
解释：答案为 B。

80. 为了进一步提高信息安全的保障能力和防护水平，保障和促进信息化建设的健康发展，公安部等 4 部分联合发布《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)，对等级保护工作的开展提供宏观指导和约束，明确了等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责分工等，关于该文件，下面理解正确的是
A.该文件时一个由部委发布的政策性文件，不属于法律文件
B.该文件适用于 2004 年的等级保护工作，其内容不能越苏到 2005 年及之后的工作
C.该文件时一个总体性知道文件，规定了所有信息系统都要纳入等级保护定级范围
D.该文件使用范围为发文的这四个部门，不适用于其他部门和企业等单位
解释：答案为 A。

81. 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”中进行一步细化和扩展
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
解释：ITSEC 最早强调功能和保证的分离，不是 CC 的先进性。

82. 对于数字证书而言，一般采用的是哪个标准？
A.ISO/IEC 1540B B.802.11 C.GB/T 20984 D.X.509
解释：答案为 D。

83. 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
解释：答案为 B1。

84. 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发生冲突，应以国际标准条款为准。
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，冰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。
解释：当国家标准和国际标准的条款发生冲突，应以国家标准条款为准。

85. 2005 年，RFC4301（Request for Comments 4301：Security Architecture for the Intermet Protocol）发布，用以取代原先的 RFC2401，该标准建议规定了 IPsec 系统基础架构，描述如何在 IP 层（IPv4/IPv6）为流量提供安全业务，请问此类 RFC 系列标准建设是由哪个组织发布的（）
A.国际标准化组织 B.国际电工委员会
C.国际电信联盟远程通信标准化组织 D.Internet 工程任务组（IETF）

解释：D 为正确答案。

86. 关于信息安全管理体系，国际上有标准（ISO/IEC 27001:2013）而我国发布了《信息技术安全技术信息安全管理体系要求》(GB/T 22080-2008）请问，这两个标准的关系是：
A.IDT (等同采用)，此国家标准等同于该国际标准，仅有或没有编辑性修改
B.EQV(等效采用)，此国家标准不等效于该国际标准
C.NEQ（非等效采用），此国家标准不等效于该国际标准
D.没有采用与否的关系，两者之间版本不同，不应该直接比较
解释：ISO/IEC 27001:2013 和 GB/T 22080-2008 是两个不同的版本。

87. GB/T18336<<信息技术安全性评估准则>>（CC）是测评标准类中的重要标准，该标准定义了保护轮廓（Protection Profile ，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）,其评估保证级共分为（）个递增的评估保证等级
A.4 B.5 C.6 D.7
解释：CC 标准 EAL1-EAL7 级。

88. 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
解释：A 为监理的内容。

89. 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
解释：网络空间安全不能单纯依靠技术措施来保障。

90. 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 C.成本控制由承建单位实现，监理单位只能记录实际开销
B.成本应控制得越低越好 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
解释：D 为正确答案。

91. 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
解释：SSE-CMM 用于对安全建设工程的成熟度进行评估。CC 是信息技术产品或系统的规划、设计、研发、测试、EAL 级别评估进行使用。

92. 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》
解释：B 为正确答案。

93. ISO／IEC27001《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》 C. 信息技术安全评估准则(简称 ITSEC)
B. BS7799-2《信息安全管理体系规范》 D. 信息技术安全评估通用标准(简称 CC)
解释：BS7799-1 发展为 ISO27002；BS7799-2 发展为 ISO27001；TCSEC 发展为 ITSEC；ITSEC 发展为 CC。

94. 在 GB／T18336《信息技术安全性评估准则》(CC 标准）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 C.两份不同的 ST 不可能满足同一份 PP 的要求
B.PP 描述的安全要求与具体实现无关 D.ST 与具体的实现有关

解释：两份不同的 ST 可以同时满足同一份 PP 的要求。

95. 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
解释：提高信息技术产品的国产化率不属于九项重点工作内容之一。

96. 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
解释：A 为概念与需求定义的工作内容。B 是安全规划设计阶段内容。C 是实施阶段。D 是验收测试阶段的内容。

97. 以下关于法律的说法错误的是（）
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”
解释：法律是公开的，内部的规定不能作为法律。

98. 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，今早发现软件安全问题
解释：开发人员采用敏捷开发模型进行软件开发，但未包括安全的开发方法和措施。

99. 根据信息安全风险要素之间的关系，下图中空白处应该填写（）

A.资产 B、安全事件 C、脆弱性 D、安全措施
解释：风险的原理是威胁利用脆弱性，造成对资产的风险。

100. 信息安全标准化工作是我国信息安全保障工作的重要组成部分之一，也是政府进行宏观管理的重要依据，同时也是保护国家利益，促进产业发展的重要手段之一，关于我国标准化工作，下面选项中**描述错误**的是（）
A、我国是在国家质量监督检验疫总局管理下，由国家标准化管理委员会统一管理全国标准化工作，下设专业技术委员会
B、事关国家安全利益，信息安全因此不能和国际标准相同，而是要通过本国组织和专家制定标准，切实有效地保护国家利益和安全
C、我国归口信息安全方面标准是“全国信息安全标准化技术委员会”，为加强有关工作，2016 在其下设立“大数据安全特别工作组”
D、信息安全标准化工作是解决信息安全问题的重要技术支撑，其主要作业突出体现在能够确保有关产品、设施的技术先进性、可靠性和一致性
解释：信息安全的标准可以和国际标准相同，也可以不相同。包括同等采用方式和等效采用方式等。