中国信息安全测评中心 CISP 认证
模拟试题

中电运行信息安全网络技术测评中心　编辑

1.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

2.以下哪一项不是《GB/T20274 信息安全保障评估框架》给出的信息安全保障模型具备的特点？

A．强调信息系统安全保障持续发展的动态性，即强调信息系统安全保障应贯穿于整个信息系统生命周期的全过程

B．强调信息系统安全保障的概念，通过综合技术、管理、工程和人员的安全保障要求来实施和实现信息系统的安全保障目标

C．以安全概念和关系为基础，将安全威胁和风险控制措施作为信息系统安全保障的基础和核心

D．通过以风险和策略为基础，在整个信息系统的生命周期中实施技术、管理、工程和人员保障要素，从而使信息系统安全保障实现信息安全的安全特征

3.以下关于信息系统安全保障是主观和客观的结合说法最准确的是：

A．信息系统安全保障不仅涉及安全技术，还应综合考虑安全管理、安全工程和人员安全等，以全面保障信息系统安全

B．通过技术、管理、工程和人员方面客观地评估安全保障措施，向信息系统的所有者提供其现有安全保障工作是否满足其安全保障目标的信心

C．是一种通过客观证据向信息系统评估者提供主观信心的活动

D．是主观和客观综合评估的结果

4.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

5.在密码学的 Kerchhoff 假设中，密码系统的安全性仅依赖于_____。

A．明文

B．密文

C．密钥

D．信道

6.通过对称密码算法进行安全消息传输的必要条件是：

A．在安全的传输信道上进行通信

B．通讯双方通过某种方式，安全且秘密地共享密钥

C．通讯双方使用不公开的加密算法

D．通讯双方将传输的信息夹杂在无用信息中传输并提取

7.以下关于代替密码的说法正确的是：

A．明文根据密钥被不同的密文字母代替
B．明文字母不变，仅仅是位置根据密钥发生改变
C．明文和密钥的每个 bit 异或
D．明文根据密钥作移位

8.AES 在抵抗差分密码分析及线性密码分析的能力比 DES 更有效，已经替代 DES 成为新的数据加密标准。其算法的信息块长度和加密密钥是可变的，以下哪一种不是其可能的密钥长度？
A．64bit
B．128bit
C．192bit
D．256bit

9.Alice 有一个消息 M 通过密钥 K2 生成一个密文 E（K2，M）然后用 K1 生成一个 MAC 为 C（K1，E（K2，M）），Alice 将密文和 MAC 发送给 Bob，Bob 用密钥 K1 和密文生成一个 MAC 并和 Alice 的 MAC 比较，假如相同再用 K2 解密 Alice 发送的密文，这个过程可以提供什么安全服务？
A．仅提供数字签名
B．仅提供保密性
C．仅提供不可否认性
D．保密性和消息完整性

10.PKI 在验证一个数字证书时需要查看-_____，来确认该证书是否已经作废。
A．ARL
B．CSS
C．KMS
D．CRL

11.时间戳的引入主要是为了防止：
A．死锁
B．丢失
C．重放
D．拥塞

12.以下对于安全套接层（SSL）的说法正确的是：
A．主要是使用对称密钥体制和 X509 数字证书技术保护信息传输的机密性和完整性
B．可以在网络层建立 VPN
C．主要适用于点对点之间的信息传输，常用 WebServer 方式
D．包含三个主要协议：AH、ESP、IKE

13.按照 BLP 模型规则，以下哪种访问不能被授权：
A．Bob 的安全级是（机密，{NUC，EUR}），文件的安全级是（机密，{NUC，EUR，AMC}），Bob 请求写该文件
B．Bob 的安全级是（机密，{NUC，EUR}），文件的安全级是（机密，{NUC}），Bob 请求读该文件

C．Alice 的安全级是（机密，{NUC，EUR}），文件的安全级是（机密，{NUC，US}），Alice 请求写该文件

D．Alice 的安全级是（机密，{NUC，US}），文件的安全级是（机密，{NUC，US}），Alice 请求读该文件

14.为了防止授权用户不会对数据进行未经授权的修改，需要实施对数据的完整性保护，下列哪一项最好地描述了星或（*-）完整性原则？

A．Bell-LaPadula 模型中的不允许向下写

B．Bell-LaPadula 模型中的不允许向上读

C．Biba 模型中的不允许向上写

D．Biba 模型中的不允许向下读

15.下面哪一个情景属于身份鉴别（Authentication）过程？

A．用户依照系统提示输入用户名和口令

B．用户在网络上共享了自己编写的一份 Office 文档，并设定哪些用户可以阅读，哪些用户可以修改

C．用户使用加密软件对自己编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后看到文档中的内容

D．某个人尝试登陆到你的计算机中，但是口令输入的不对，系统提示口令错误，并将这次失败的登陆过程纪录在系统日志中

16.下列对 Kerberos 协议特点描述不正确的是：

A．协议采用单点登录技术，无法实现分布式网络环境下的认证

B．协议与授权机制相结合，支持双向的身份认证

C．只要用户拿到了 TGT 并且该 TGT 没有过期，就可以使用该 TGT 通过 TGS 完成到任一个服务器的认证而不必重新输入密码

D．AS 和 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

17.TACACS+协议提供了下列哪一种访问控制机制？

A．强制访问控制

B．自主访问控制

C．分布式访问控制

D．集中式访问控制

18.令牌（Tokens），智能卡及生物检测设备同时用于识别和鉴别，依据的是以下哪个原则？

A．多因素鉴别原则

B．双因素鉴别原则

C．强制性鉴别原则

D．自主性鉴别原则

19.下列对密网功能描述不正确的是：

A．可以吸引或转移攻击者的注意力，延缓他们对真正目标的攻击

B．吸引入侵者来嗅探、攻击，同时不被觉察地将入侵者的活动记录下来
C．可以进行攻击检测和实时报警
D．可以对攻击活动进行监视、检测和分析

20.下列对审计系统基本组成描述正确的是：
A．审计系统一般包含三个部分：日志记录、日志分析和日志处理
B．审计系统一般包含两个部分：日志记录和日志处理
C．审计系统一般包含两个部分：日记记录和日志分析
D．审计系统一般包含三个部分：日志记录、日志分析和日志报告

21.安全审计是对系统活动和记录的独立检查和验证，以下哪一项不是审计系统的作用：
A．辅助辨识和分析未经授权的活动或攻击
B．对与已建立的安全策略的一致性进行核查
C．及时阻断违反安全策略的访问
D．帮助发现需要改进的安全控制措施

22.UDP 需要使用_____地址，来给相应的应用程序发送用户数据报。
A．端口
B．应用程序
C．因特网
D．物理

23.下面对 WAPI 描述不正确的是：
A．安全机制由 WAI 和 WPI 两部分组成
B．WAI 实现对用户身份的鉴别
C．WPI 实现对传输的数据加密
D．WAI 实现对传输的数据加密

24.通常在设计 VLAN 时，以下哪一项不是 VLAN 的规划的方法？
A．基于交换机端口
B．基于网络层协议
C．基于 MAC 地址
D．基于数字证书

25.某个客户的网络现在可以正常访问 Internet 互联网，共有 200 台终端 PC 但此客户从 ISP（互联网络服务提供商）里只获得了 16 个公有的 IPv4 地址，最多也只有 16 台 PC 可以访问互联网，要想让全部 200 台终端 PC 访问 Internet 互联网最好采取什么方法或技术：
A．花更多的钱向 ISP 申请更多的 IP 地址
B．在网络的出口路由器上做源 NAT
C．在网络的出口路由器上做目的 NAT
D．在网络的出口处增加一定数量的路由器

26.路由器的标准访问控制列表以什么作为判别条件
A．数据包的大小

B．数据包的源地址
C．数据包的端口号
D．数据包的目的地址

27.桥接或透明模式是目前比较流行的防火墙部署方式，这种方式的优点不包括：
A．不需要对原有的网络配置进行修改
B．性能比较高
C．防火墙本身不容易受到攻击
D．易于在防火墙上实现 NAT

28.下面哪一项是对 IDS 的正确描述？
A．基于特征（Signature-based）的系统可以检测新的攻击类型
B．基于特征（Signature-based）的系统比基于行为（behavior-based）的系统产生更多的误报
C．基于行为（behavior-based）的系统维护状态数据库来与数据包和攻击相匹配
D．基于行为（behavior-based）的系统比基于特征（Signature-based）的系统有更高的误报

29.下列哪些选项不属于 NIDS 的常见技术？
A．协议分析
B．零拷贝
C．SYNCookie
D．IP 碎片从重组

30.以下关于 Linux 超级权限的说明，不正确的是
A．一般情况下，为了系统安全，对于一般常规级别的应用，不需要 root 用户来操作完成
B．普通用户可以通过 su 和 sudo 来获得系统的超级权限
C．对系统日志的管理，添加和删除用户等管理工作，必须以 root 用户登录才能进行
D．root 是系统的超级用户，无论是否为文件和程序的所有者都具有访问权限

31.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-x3useradmin1024Sep1311:58test
B．drwxr-xr-x3useradmin1024Sep1311:58test
C．rwxr-xr-x3adminuser1024Sep1311:58test
D．drwxr-xr-x3adminuser1024Sep1311:58test

32.Windows 系统下，哪项不是有效进行共享安全的防护措施？
A．使用 netshare\\127.0.0.1\c$/delete 命令，删除系统中的 c$等管理共享，并重启系统
B．确保所有的共享都有高强度的密码防护
C．禁止通过“空会话”连接以匿名的方式列举用户、群组、系统配置和注册表键值
D．安装软件防火墙阻止外面对共享目录的连接

33.以下对 Windows 账号的描述，正确的是：
A．Windows 系统是采用 SID（安全标识符）来标识用户对文件或文件夹的权限
B．Windows 系统是采用用户名来标识用户对文件或文件夹的权限

C．Windows 系统默认会生成 administrator 和 guest 两个账号，两个账号都不允许改名和删除
D．Windows 系统默认生成 administrator 和 guest 两个账号，两个账号都可以改名和删除

34.以下对 Windows 系统的服务描述，正确的是：
A．Windows 服务必须是一个独立的可执行程序
B．Windows 服务的运行不需要用户的交互登陆
C．Windows 服务都是随系统启动而启动，无需用户进行干预
D．Windows 服务都需要用户进行登陆后，以登录用户的权限进行启动

35.以下哪一项不是 IIS 服务器支持的访问控制过渡类型？
A．网络地址访问控制
B．Web 服务器许可
C．NTFS 许可
D．异常行为过滤

36.为了实现数据库的完整性控制，数据库管理员应向 DBMS 提出一组完整性规则来检查数据库中的数据，完整性规则主要由三部分组成，以下哪一个不是完整性规则的内容？
A．完整性约束条件
B．完整性检查机制
C．完整性修复机制
D．违约处理机制

37.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

38.下列哪一项与数据库的安全有直接关系？
A．访问控制的粒度
B．数据库的大小
C．关系表中属性的数量
D．关系表中元组的数量

39.专门负责数据库管理和维护的计算机软件系统称为：
A．SQL-MS
B．INFERENCECONTROL
C．DBMS
D．TRIGGER-MS

40.电子邮件客户端通常需要用_____协议来发送邮件。
A．仅 SMTP
B．仅 POP
C．SMTP 和 POP

D．以上都不正确

41.ApacheWeb 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．srm.conf
C．access.conf
D．inetd.conf

42.为了增强电子邮件的安全性，人们经常使用 PGP，它是：
A．一种基于 RSA 的邮件加密软件
B．一种基于白名单的反垃圾邮件软件
C．基于 SSL 和 VPN 技术
D．安全的电子邮箱

43.恶意代码采用加密技术的目的是：
A．加密技术是恶意代码自身保护的重要机制
B．加密技术可以保证恶意代码不被发现
C．加密技术可以保证恶意代码不被破坏
D．以上都不正确

44.恶意代码反跟踪技术描述正确的是：
A．反跟踪技术可以减少被发现的可能性
B．反跟踪技术可以避免所有杀毒软件的查杀
C．反跟踪技术可以避免恶意代码被清除
D．以上都不正确

45.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

46.当用户输入的数据被一个解释器当作命令或查询语句的一部分执行时，就会产生哪种类型的漏洞？
A．缓冲区溢出
B．设计错误
C．信息泄露
D．代码注入

47.完整性检查和控制的防范对象是_____，防止它们进入数据库。
A．不合语义的数据，不正确的数据
B．非法用户
C．非法操作

D．非法授权

48.存储过程是 SQL 语句的一个集合，在一个名称下存储，按独立单元方式执行。以下哪一项不是使用存储过程的优点：
A．提高性能，应用程序不用重复编译此过程
B．降低用户查询数量，减轻网络拥塞
C．语句执行过程中如果中断，可以进行数据回滚，保证数据的完整性和一致性
D．可以控制用户使用存储过程的权限，以增强数据库的安全性

49.下列哪些措施不是有效的缓冲区溢出的防护措施？
A．使用标准的 C 语言字符串库进行操作
B．严格验证输入字符串长度
C．过滤不合规则的字符
D．使用第三方安全的字符串库操作

50.以下工作哪个不是计算机取证准备阶段的工作
A．获得授权
B．准备工具
C．介质准备
D．保护数据

51.以下哪个问题不是导致 DNS 欺骗的原因之一？
A．DNS 是一个分布式的系统
B．为提高效率，DNS 查询信息在系统中会缓存
C．DNS 协议传输没有经过加密的数据
D．DNS 协议是缺乏严格的认证

52.以下哪个是 ARP 欺骗攻击可能导致的后果？
A．ARP 欺骗可直接获得目标主机的控制权
B．ARP 欺骗可导致目标主机的系统崩溃，蓝屏重启
C．ARP 欺骗可导致目标主机无法访问网络
D．ARP 欺骗可导致目标主机死机

53.以下哪个攻击步骤是 IP 欺骗（IPSpoof）系列攻击中最关键和难度最高的？
A．对被冒充的主机进行拒绝服务攻击，使其无法对目标主机进行响应
B．与目标主机进行会话，猜测目标主机的序号规则
C．冒充受信主机向目标主机发送数据包，欺骗目标主机
D．向目标主机发送指令，进行会话操作

54.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．UDPFlood
C．Smurf
D．Teardrop

55.如果一名攻击者截获了一个公钥，然后他将这个公钥替换为自己的公钥并发送给接收者，这种情况属于哪一种攻击？
A．重放攻击
B．Smurf 攻击
C．字典攻击
D．中间人攻击

56.域名注册信息可在哪里找到？
A．路由表
B．DNS 记录
C．whois 数据库
D．MIBs 库

57.网络管理员定义“noipdirectedbroadcast”以减轻下面哪种攻击？
A．Diecast
B．Smurf
C．Batcast
D．Coke

58.下面哪一项不是黑客攻击在信息收集阶段使用的工具或命令：
A．Nmap
B．Nslookup
C．LC
D．Xscan

59.下面关于软件测试的说法错误的是：
A．所谓“黑盒”测试就是测试过程不测试报告中进行描述，且对外严格保密
B．出于安全考虑，在测试过程中尽量不要使用真实的生产数据
C．测试方案和测试结果应当成为软件开发项目文档的主要部分被妥善的保存
D．软件测试不仅应关注需要的功能是否可以被实现，还要注意是否有不需要的功能被实现了

60.以下哪个不是 SDL 的思想之一：
A．SDL 是持续改进的过程，通过持续改进和优化以适用各种安全变化，追求最优效果
B．SDL 要将安全思想和意识嵌入到软件团队和企业文化中
C．SDL 要实现安全的可度量性
D．SDL 是对传统软件开发过程的重要补充，用于完善传统软件开发中的不足

61.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地网络信息流时，这种攻击称之为：
A．Land 攻击
B．Smurf 攻击
C．PingofDeath 攻击
D．ICMPFlood

62.以下哪种方法不能有效提高 WLAN 的安全性：
A．修改默认的服务区标识符（SSID）
B．禁止 SSID 广播
C．启用终端与 AP 间的双向认证
D．启用无线 AP 的开放认证模式

63.以下哪项是对抗 ARP 欺骗有效的手段？
A．使用静态的 ARP 缓存
B．在网络上阻止 ARP 报文的发送
C．安装杀毒软件并更新到最新的病毒库
D．使用 Linux 系统提高安全性

64.以下关于 ISO/IEC27001 标准说法不正确的是：
A．本标准可被内部和外部相关方用于一致性评估，审核的重点就是组织信息安全的现状，对部属的信息安全控制是好的还是坏的做出评判
B．本标准采用一种过程方法来建立、实施、运行、监视、评审、保持和改进一个组织的 ISMS
C．目前国际标准化组织推出的四个管理体系标准：质量管理体系，职业健康安全管理体系、环境管理体系、信息安全管理体系，都采用了相同的方法，即 PDCA 模型
D．本标准注重监视和评审，因为监视和评审是持续改进的基础，如果缺乏对执行情况和有效性的测量，改进就成了“无的放矢”

65.下列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

66.下列安全控制措施的分类中，哪个分类是正确的（P-预防性的，D-检测性的以及 C-纠正性的控制）：
1.网络防火墙
2.RAID 级别 3
3.银行账单的监督复审
4.分配计算机用户标识
5.交易日志
A.)P，P，C，D，andC
B.)D，C，C，D，andD
C.)P，C，D，P，andD
D.)P，D，P，P，andC

67.风险评估主要包括风险分析准备、风险要素识别、风险分析和风险结果判定四个主要过程，关于这些过程，以下的说法哪一个是正确的？
A．风险分析准备的内容是识别风险的影响和可能性
B．风险要素识别的内容是识别可能发生的安全事件对信息系统的影响程度

C．风险分析的内容是识别风险的影响和可能性
D．风险结果判定的内容是发生系统存在的威胁、脆弱性和控制措施

68.你来到服务器机房隔壁的一间办公室，发现窗户坏了。由于这不是你的办公室，你要求在这里办公的员工请维修工来把窗户修好。你离开后，没有再过问这扇窗户的事情。
这件事的结果对与特定脆弱性相关的威胁真正出现的可能性会有什么影响？
A．如果窗户被修好，威胁真正出现的可能性会增加
B．如果窗户被修好，威胁真正出现的可能性会保持不变
C．如果窗户没有被修好，威胁真正出现的可能性会下降
D．如果窗户没有被修好，威胁真正出现的可能性会增加

69.在对安全控制进行分析时，下面哪个描述是不准确的？
A．对每一项安全控制都应该进行成本收益分析，以确定哪一项安全控制是必须的和有效的
B．应确保选择对业务效率影响最小的安全措施
C．选择好实施安全控制的时机和位置，提高安全控制的有效性
D．仔细评价引入的安全控制对正常业务带来的影响，采取适当措施，尽可能减少负面效应

70.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

71.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

72.以下哪一项不是建筑物的自动化访问审计系统记录的日志的内容：
A．出入的原因
B．出入的时间
C．出入口的位置
D．是否成功进入

73.信息安全策略是管理层对信息安全工作意图和方向的正式表述，以下哪一项不是信息安全策略文档中必须包含的内容：
A．说明信息安全对组织的重要程度
B．介绍需要符合的法律法规要求
C．信息安全技术产品的选型范围
D．信息安全管理责任的定义

74.作为信息中心的主任，你发现没有足够的人力资源保证将数据库管理员和网络管理员的岗位

分配给两个不同的人担任，这种情况造成了一定的安全风险，这时你应当怎么做？
A．抱怨且无能为力
B．向上级报告该情况，等待增派人手
C．通过部署审计措施和定期审查来降低风险
D．由于增加人力会造成新的人力成本，所以接受该风险

75.以下人员中，谁负有决定信息分类级别的责任？
A．用户
B．数据所有者
C．审计员
D．安全员

76.某公司正在对一台关键业务服务器进行风险评估：该服务器价值 138000 元，针对某个特定威胁的暴露因子（EF）是 45%，该威胁的年度发生率（ARO）为每 10 年发生 1 次。根据以上信息，该服务器的年度预期损失值（ALE）是多少？
A．1800 元
B．62100 元
C．140000 元
D．6210 元

77.下列哪些内容应包含在信息系统战略计划中？
A．已规划的硬件采购的规范
B．将来业务目标的分析
C．开发项目的目标日期
D．信息系统不同的年度预算目标

78.ISO2002 中描述的 11 个信息安全管理控制领域不包括：
A．信息安全组织
B．资产管理
C．内容安全
D．人力资源安全

79.依据国家标准《信息安全技术信息系统灾难恢复规范》(GB/T20988)，需要备用场地但不要求部署备用数据处理设备的是灾难恢复等级的第几级？
A．2
B．3
C．4
D．5

80.以下哪一种备份方式在恢复时间上最快？
A．增量备份
B．差异备份
C．完全备份
D．磁盘镜像

81.计算机应急响应小组的简称是？
A．CERT
B．FIRST
C．SANA
D．CEAT

82.有一些信息安全事件是由于信息系统中多个部分共同作用造成的，人们称这类事件为“多组件事故”，应对这类安全事件最有效的方法是：
A．配置网络入侵检测系统以检测某些类型的违法或误用行为
B．使用防病毒软件，并且保持更新为最新的病毒特征码
C．将所有公共访问的服务放在网络非军事区（DMZ）
D．使用集中的日志审计工具和事件关联分析软件

83.依据国家标准《信息安全技术信息系统灾难恢复范围》（GB/T20988），灾难恢复管理过程的主要步骤是灾难恢复需求分析、灾难恢复策略制定、灾难恢复策略实现、灾难恢复预案制定和管理；其中灾难恢复策略实现不包括以下哪一项？
A．分析业务功能
B．选择和建设灾难备份中心
C．实现灾备系统技术方案
D．实现灾备系统技术支持和维护能力

84.拒绝服务攻击导致的危害中，以下哪个说法是不正确的：
A．网络带宽被耗尽，网络被堵塞，无法访问网络
B．主机资源被耗尽，主机无法响应请求
C．应用资源被耗尽，应用无法响应请求
D．应用系统被破坏，应用无法响应请求

85.SSE-CMM 将工程过程区域分为三类，即风险过程、工程过程、和保证过程，下面对于保证过程的说法错误的是：
A．保证是指安全需求得到满足的可信任程度
B．信任程度来自于对安全工程过程结果质量的判断
C．自验证与证实安全的主要手段包括观察、论证、分析和测试
D．PA“建立保证论据”为 PA“验证与证实安全”提供了证据支持

86.根据 SSE-CMM 信息安全工程过程可以划分为三个阶段，其中_____确立安全解决方案的置信度并且把这样的置信度传递给顾客。
A．保证过程
B．风险过程
C．工程和保证过程
D．安全工程过程

87.SSE-CMM 工程过程区域中的风险过程包含哪些过程区域：
A．评估威胁、评估脆弱性、评估影响
B．评估威胁、评估脆弱性、评估安全风险

C．评估威胁、评估脆弱性、评估影响、评估安全风险
D．评估威胁、评估脆弱性、评估影响、验证和证实安全

88.一个组织的系统安全能力成熟度达到哪个级别以后，就可以对组织层面的过程进行规范的定义？
A．2 级——计划和跟踪
B．3 级——充分定义
C．4 级——量化控制
D．5 级——持续改进

89.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善
D．通过测试证明系统的功能和性能可以满足安全要求

90.信息化建设和信息安全建设的关系应该是：
A．信息化建设的结果就是信息安全建设的开始
B．信息化建设和信息安全建设应同步规划、同步实施
C．信息化建设和信息安全建设是交替进行的，无法区分谁先谁后
D．以上说法都正确

91.如果你作为甲方负责监督一个信息安全工程项目的实施，当乙方提出一项工程变更时你最应当关注的是：
A．变更的流程是否符合预先的规定
B．变更是否会对项目进度造成拖延
C．变更的原因和造成的影响
D．变更后是否进行了准确的记录

92.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

93.在进行应用系统的测试时，应尽可能避免使用包含个人隐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

94.下面有关我国信息安全管理体制的说法错误的是？
A．目前我国的信息安全保障工作是相关部门各司其职、相互配合、齐抓共管的局面
B．我国的信息安全保障工作综合利用法律、管理和技术的手段
C．我国的信息安全管理应坚持及时检测、快速响应、综合治理的方针
D．我国对于信息安全责任的原则是谁主管、谁负责；谁经营、谁负责

95.下列关于 ISO15408 信息技术安全评估准则（简称 CC）通用性的特点，即给出通过的表达方式，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

96.TCSEC（橘皮书）中划分的 7 个安全等级中，_____是安全程度最高的安全等级
A．A1
B．A2
C．C1
D．C2

97.对第三方服务进行安全管理时，以下说法正确的是：
A．服务水平协议的签定可以免除系统安全管理者的责任
B．第三方服务的变更管理的对象包括第三方服务造成的系统变化和服务商自身的变化
C．服务水平协议的执行情况的监督，是服务方项目经理的职责，不是系统安全管理者的责任
D．安全加固的工作不能由第三方服务商进行

98.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》

99.以下哪一项是用于 CC 的评估级别？
A．EAL1，EAL2，EAL3，EAL4，EAL5，EAL6，EAL7
B．A1，B1，B2，B3，C2，C1，D
C．E0，E1，E2，E3，E4，E5，E6
D．AD0，AD1，AD2，AD3，AD4，AD5,AD6

100.我国信息安全标准化技术委员会（TC260）目前下属 6 个工作组，其中负责信息安全管理的小组是：
A．WG1
B．WG7

C．WG3
D．WG5

101.下面关于信息安全保障的说法正确的是:
A.信息安全保障的概念是与信息安全的概念同时产生的
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
C.信息安全保障和信息安全技术并列构成实现信息安全的两大主要手段
D.信息安全保障是以业务目标的实现为最终目的，从风险和策略出发，实施各种保障要素，在系统的生命周期内确保信息的安全属性

102.以下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帐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

103.依据国家标准 GB/T20274《信息系统安全保障评估框架》，信息系统安全目标(ISST)是从信息系统安全保障_____的角度来描述的信息系统安全保障方案。
A.建设者
B.所有者
C.评估者
D.创定者

104.常见密码系统包含的元素是：
A.明文，密文，信道，加密算法，解密算法
B.明文，摘要，信道，加密算法，解密算法
C.明文，密文，密钥，加密算法，解密算法
D.消息，密文，信道，加密算法，解密算法

105.下列哪一项功能可以不由认证中心 CA 完成?
A.撤销和中止用户的证书
B.产生并分发 CA 的公钥
C.在请求实体和它的公钥间建立链接
D.发放并分发用户的证书
106.下列哪一项是虚拟专用网络（VPN）的安全功能
A.验证，访问控制和密码
B.隧道，防火墙和拨号
C.加密，鉴别和密钥管理
D.压缩，解密和密码

107.下列对审计系统基础基本组成描述正确的是：
A.审计系统一般包括三个部分：日志记录、日志分析和日志处理
B.审计系统一般包括两个部分：日志记录和日志处理

C.审计系统一般包括两个部分：日志记录和日志分析
D.审计系统一般包括三个部分：日志记录、日志分析和日志报告

108.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，以下那一层次提供保密性、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

109.以下哪个一项数据传输方式难以通过网络窃听获取信息？
A.FTP 传输文件
B.TELNET 进行远程管理
C.URL 以 HTTPS 开头的网页内容
D.经过 TACACS+认证和授权后建立的链接

110.在 Unix 系统中输入命令“is 一 altest”显示如下
"-rwxr-xr-x3rootroot1024Sep1311:58test"
对它的含义解释错误的是:
A.这是一个文件，而不是目录
B.的拥有者可以对这个文件进行读、写和执行的操作
C.文件所属组的成员有可以读它，也可以执行它
D.其它所有用户只可以执行它

111..在 Unix 系统中，/etc/service 文件记录 T 什么内容?
A.记录一些常用的接口及其所提供的服务的对应关系
B.决定 inetd 启动网络服务时，启动哪些服务
C.定义了系统缺省运行级别，系统进入新运行级别需要做什么
D.包含了系统的一些启动脚本

112.数据库事务日志的用途是什么？
A.事务处理
B.效据恢复
C.完整性约束
D.保密性控制
113.以下哪一项是和电子邮件系统无关的？
A.PEM(Privacyenhancedmail)
B.PGP(P rettygoodPrivacy)
C.X.500
D.X.400

114.城名注册信息可在哪里找到?
A.路由表
B.DNS 记录

C.whois 数据库
D.MIBs 库

115.网络普理员定义“noipdirectedbroadcast”以减轻下面哪种攻击?
A.Diecast
B.Smurf
C.Batcast
D.Coke

116.下列哪一项不属于 Fuzz 测试的特性
A.主要针对软件漏洞或可靠性错误进行测试
B.采用大量测试用例进行漏洞-相应测试
C.一种试探性测试方法，没有任何理论依据
D.利用构造畸形的输入数据引发被测试目标产生异常

117..风险评估方法的选定在 PDCA 循环中的哪个阶段完成？
A.实施和运行
B.保持和改进
C.建立
D.监视和评审

118.下面关于 ISO27002 的说法错误的是：
A.ISO27002 的前身是 ISO17799-1
B.ISO27002 给出了通常意义下的信息安全管理最佳实践供组织机构选用，但不是全部
C.ISO27002 对于每个控制措施的表述分“控制措施”、“实施指南”和“其他信息”三个部分来进行描述
D.ISO27002 提出了十一大类的安全管理措施，其中风险评估和处置是处于核心地位的一类安全措施

119.在风险管理准备阶段“建立背景”（对象确立）过程中不应该做的是：
A.分析系统的体系结构
B.分析系统的安全环境
C.制定风险管理计划
D.调查系统的技术特性

120.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：
A 设置网络链接时限
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

121.以下选项中哪一项是对于信息安全风险采取的纠正机制
A 访问控制
B 入侵检测

C.灾难恢复
D 防病毒系统

122.你来到服务器机房隔壁一间办公室，发现窗户坏了。由于这不是你的办公室，你要求在这里办公的员工请维修工来把窗户修好。你离开后，没有再过问这窗户的事情。这件事的结果对与特定脆弱性相关的威胁真正出现的可能性会有什么影响？
A.如果窗户被修好，威胁真正的出现的可能性会增加
B.如果窗户被修好，威胁真正的出现的可能性会保持不变
C.如果窗户没被修好，威胁真正的出现的可能性会下降
D.如果窗户没被修好，威胁真正的出现的可能性会增加

123.为了保护系统日志可靠有效，以下哪一项不是日志必需具备的特征：
A.统一面精确地的时间
B.全面覆盖系统资产
C.包括访问源、访问日志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

124.下面有关能力成熟度模型的说法错误的是:
A.能力成熟度模型可以分为过程能力方案（Continuous）和组织能力方案（Staged）两类
B.使用过程能力方案时，可以灵活选择评估和改进哪个或哪些过程域
C.使用组织机构成熟度方案时，每一个能力级别都对应于一组已经定义好的过程域
D.SSE-CMM 是一种属于组织能力方案（Staged）的针对系统安全工程的能力成熟度模型

125.下列哪项不是信息系统安全工程能力成熟度模型(SSE-CMM)的主要过程:
A.风险过程
B.保证过程
C.工程过程
D.评估过程

126.信息化建设和信息安全建设的关系应当是:
A.信息化建设的结束就是信息安全建设的开始
B.信息化建设和信息安全建设应同步规划、同步实施
C.信息化建设和信息安全建设是交替进行的，无法区分谁先谁后
D.以上说法都正确

127.信息安全工程监理模型不包括下面哪一项?
A.监理咨询服务
B.咨询监理支撑要素
C.监理咨询阶段过程
D.控制管理措施

128.下面有关我信息安全管理体制的说法错误的是?
A.目前我国的信息安全保障工作是相关部门各司其职、相互配合、齐抓共管的局面
B.我国的信息安全保障工作综合利用法律、管理和技术的手段

C.我国的信息安全管理应坚持及时检测、快速响应、综合治理的方针
D.我国对于信息安全贵任的原则是谁主管、谁负责；谁经营、谁负责

129.下列哪项不是安全管理方面的标准?
A.ISO27001
B.ISO13335
C.GB/T22080
DGB/T18336

130.关于 ISO/IEC21827:2002(SSE-CMM)描述不正确的是_?
A.SSE-CMM 是关于信息安全建设工程实施方面的标准。
B.SSE 一 MM 的目的是建立和完善一套成熟的、可度量的安全工程过程.
C.SSE-CMM 模型定义了一个安全工程应有的特征，这些特征是完善的安全工程的根本保证。
D.SSE-CMM 是用于对信息系统的安全等级进行评估的标准。

131.《刑法》第六章第 285.286,287 条对计算机犯罪的内容和量刑进行了明确的规定，以下哪一项不是其中规定的罪行?
A.非法侵入计算机信息系统罪
B.破坏计算机信息系统罪
C.利用计算机实施犯罪
D.国家重要信息系统管理者玩忽职守罪

132.计算机取证的合法原则是:
A.计算机取证的目的是获取证据，因此首先必须确保证据获取再履行相关法律手续
B.计算机取证在任何时候都必须保证符合相关法律法规
C.计算机取证只能由执法机构才能执行，以确保其合法性
D.计算机取证必须获得执法机关的授权才可进行以确保合法性原则

133.等级保护定级阶段主要包括哪两个步骤
A.系统识别与描述、等级确定
B.系统描述、等级确定
C.系统识别、系统描述
D.系统识别与描述、等级分级

134.目前，我国信息安全管理格局是一个多方“齐抓共管”的体制，多头管理现状决定法出多门，《计算机信息系统国际联网保密管理规定》是由下列哪个部门所制定的规章制度?
A.公安部
B.国家保密局
C.工信部
D.国家密码管理委员会办公室

135.关于信息安全保障，下列说法正确的是:
A、信息安全保障是一个客观到主观的过程，即通过采取技术、管理、工程等手段，对信息资

源的保密性、完整性、可用性提供保护，从而给信息系统所有者以信心
B、信息安全保障的需求是由信息安全策略所决定的，是自上而下的一个过程，在这个过程中，决策者的能力和决心非常重要
C、信息系统安全并不追求万无一失，而是要根据资金预算，做到量力而行
D、以上说法都正确

136.人们对信息安全的认识从信息技术安全发展到信息安全保障，主要是由于:
A、为了更好地完成组织机构的使命
B、针对信息系统的攻击方式发生重大变化
C、风险控制技术得到革命性的发展
D、除了保密性，信息的完整性和可用性也引起了人们的关注

137.关于信息安全发展的几个阶段，下列说法中错误的是:
A、信息安全的发展，是伴随着信息技术的发展，为应对其面临不同的威胁而发展起来的
B、通信安全阶段中，最重要的是通过密码技术保证所传递信息的保密性完整性和可用性
C、信息安全阶段，综合了通信安全阶段和计算机安全阶段的需求
D、信息安全保障阶段，最重要的目标是保障组织机构使命(业务)的正常运行

138.按照技术能力、所拥有的资源和破坏力来排列，下列威胁中哪种威胁最大?
A、个人黑客
B、网络阻罪团伙
C、网络战士
D、商业间谍

139.信息系统安全主要从那几个方面进行评估?
A、1 个（技术）
B、2 个（技术、管理）
C、3 个（技术、管理、工程）
D、4 个（技术、管理、工程、应用）

140.完整性机制可以防范以下哪种攻击?
A、假冒源地址或用户的地址的欺骗攻击
B、抵赖做过信息的递交行为
C、数据传输中被窃听获取
D、数据传输中被篡改或破坏
141.PPOR 模型不包括:
A、策略
B、检测
C、响应
D、加密

D（这个题应该是 PPDR，也就是 P2DR 吧？怀疑）
142.据信息系统安全保障评估框架，确定安全保障需求考虑的因素不包括下面哪一方面?
A、法规政策的要求

B、系统的价值
C、系统要对抗的威胁
D、系统的技术构成

143.依据国家标准 GB/T20274《信息系统安全保障评估框架》.在信息系统安全目标中，评估对象包括哪些内容?
A、信息系统管理体系、技术体系、业务体系
B、信息系统整体、信息系统安全管理、信息系统安全技术和信息系统安全工程
C、信息系统安全管理、信息系统安全技术和信息系统安全工程
D、信息系统组织机构、管理制度、资产

144.关于信息安全保障管理体系建设所需要重点考虑的因素，下列说法错误的是:
A、国家、上级机关的相关政策法规要求
B、组织的业务使命
C、信息系统面临的风险
D、项目的经费预算

145．在密码学的 Kerchhoff 假设中，密码系统的安全性仅依赖于。
A、明文
B、密文
C、密钥
D、信道

146.公钥密码的应用不包括:
A、数字签名
B、非安全信道的密钥交换
C、消息认证码
D、身份认证

147.hash 算法的碰撞是指:
A、两个不同的消息，得到相同的消息摘要
B、两个相同的消息，得到不同的消息摘要
C、消息摘要和消息的长度相同
D、消息摘要比消息长度更长

148.DSA 算法不提供以下哪种服务?
A、数据完整性
B、加密
C、数字签名
D、认证

149.以下哪一项都不是 PKI/CA 要解决的问题:
A、可用性、身份鉴别
B、可用性、授权与访问控制

C、完整性、授权与访问控制
D、完整性、身份鉴别

150.以下关于 VPN 说法正确的是：
A、VPN 指的是用户自己租用线路，和公共网络完全隔离的、安全的线路
B、VPN 是用户通过公用网络建立的临时的安全的连接
C、VPN 不能做到信息验证和身份认证
D、VPN 只能提供身份认证、不能提供加密数据的功能

151.下面对访问控制技术描述最准确的是:
A、保证系统资源的可靠性
B、实现系统资源的可追查性
C、防止对系统资源的非授权访问
D、保证系统资源的可信性

152.下列对自主访问控制说法不正确的是:
A、自主访问控制允许客体决定主体对该客体的访问权限
B、自主访问控制具有较好的灵活性扩展性
C、自主访问控制可以方便地调整安全策略
D、自主访问控制安全性不高，常用于商业系统

153.下列对常见强制访问控制模型说法不正确的是:
A、BLP 模型影响了许多其他访问控制模型的发展
B、Clark-Wilson 模型是一种以事物处理为基本操作的完整性模型
C、ChineseWall 模型是一个只考虑完整性的安全策略模型
D、Biba 模型是-种在数学上与 BLP 模型对偶的完整性保护模型

154.以下关于 BLP 模型规则说法不正确的是:
A、BLP 模型主要包括简单安全规则和*-规则
B、*-规则可以简单表述为向下写
C、主体可以读客体，当且仅当主体的安全级可以支配客体的安全级，且主体对该客体具有自主型读权限
D、主体可以写客体，当且仅当客体的安全级可以支配主体的安全级，且主体对客体;具有自主型写权限

155.在一个使用 ChineseWall 模型建立访问控制的信息系统中，数据 W 和数据 X 在一个兴趣冲突域中，数据 Y 和数据 Z 在另一个信息兴趣冲突域中，那么可以确定一个新注册的用户：
A、只有访问了 W 之后，才可以访问 X
B、只有访问了 W 之后，才可以访问 Y 和 Z 中的一个
C、无论是否访问 W，都只能访问 Y 和 Z 中的一个
D、无论是否访问 W，都不能访问 Y 或 Z

156.以下关于 RBAC 模型的说法正确的是:
A、该模型根据用户所担任的角色和安全级来决定用户在系统中的访问权限。

B、一个用户必须扮演并激活某种角色，才能对一个对象进行访问或执行某种操作
C、在该模型中，每个用户只能有一个角色
D、在该模型中，权限与用户关联，用户与角色关联

157.以下对 Kerberos 协议过程说法正确的是：
A、协议可以分为两个步骤:一是用户身份鉴别；二是获取请求服务
B、协议可以分为两个步骤:一是获得票据许可票据；二是获取请求服务
C、协议可以分为三个步骤:一是用户身份鉴别；二是获得票据许可票据；三是获得服务许可票据
D、协议可以分为三个步骤:一是获得票据许可票据；二是获得服务许可票据；三是获得服务

158.以下对于非集中访问控制中"域"说法正确的是：
A、每个域的访问控制与其它域的访问控制相互关联
B、跨域访问不一定需要建立信任关系
C、域中的信任必须是双向的
D、域是一个共享同一安全策略的主体和客体的集合

159.以下对单点登录技术描述不正确的是:
A、单点登录技术实质是安全凭证在多个用户之间的传递或共享
B、使用单点登录技术用户只需在登录时进行一次注册，就可以访问多个应用
C、单点登录不仅方便用户使用，而且也便于管理
D、使用单点登录技术能简化应用系统的开发

160.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

161.WPA2 包含下列哪个协议标准的所有安全特性?
A、IEEE802.11b
B、IEEE802.11c
C、IEEE802.11g
D、IEEE802.11i

162.下列关于防火墙的主要功能包括:
A、访问控制
B、内容控制
C、数据加密
D、查杀病毒

163.以下哪一项不是应用层防火墙的特点。

A、更有效的阻止应用层攻击
B、工作在 0S1 模型的第七层
C、速度快且对用户透明
D、比较容易进行审计

164.下面哪项不是 IDS 的主要功能：
A、监控和分析用户和系统活动
B、统计分析异常活动模式
C、对被破坏的数据进行修复
D、识别活动模式以反映已知攻击

165.以下关于 windowsSAM(安全账号管理器)的说法错误的是:
A、安全账号管理器(SAM)具体表现就是%SystemRoot%\system32\config\sam
B、安全账号管理器(SAM)存储的账号信息是存储在注册表中
C、安全账号管理器(SAM)存储的账号信息 administrator 和 system 是可读和可写的
D、安全账号管理器(SAM)是 windows 的用户数据库系统进程通过 SecurityAccountsManager 服务进行访问和操作

166.下列哪个是病毒的特性?
A 不感染、依附性 B 不感染、独立性
C 可感染、依附性 D 可感染、独立性

167.以下哪一项不是 IIS 服务器支持的访问控制过滤类型?
A 网络地址访问控制
Bweb 服务器许可
CNTFS 许可
D 异常行为过滤

168.下列哪个是病毒的特性?
A 不感染、依附性 B 不感染、独立性
C 可感染、依附性 D 可感染、独立性

169.下列哪一项不是信息安全漏洞的载体?
A 网络协议
B 操作系统
C 应用系统
D 业务数据

170.在某个攻击中，由于系统用户或系统管理员主动泄漏，使得攻击者可以访问系统资源的行为被称作:
A 社会工程
B 非法窃取
C 电子欺骗
D 电子窃听

171.以下针对 SDL 的需求分析的描述最准确的是:
A 通过安全需求分析，确定软件安全需要的安全标准和相关要求
B 通过安全需求分析，确定软件安全需要的安全技术和工作阳呈
C 通过安全窝求分析，确定软件安全需要的安全标准和安全管理
D 通过安全需求分析，确定软件安全需要的安全技术和安全管理

172.信息安全管理者需要完成方方面面的繁杂工作，这些日常工作根本的目标是:
A 避免系统软硬件的损伤
B 监视系统用户和维护人员的行为
C 保护组织的信息资产
D 给入侵行为制造障碍，并在发生入侵后及时发现、准确记录

173.信息安全管理的根本方法是:
A 风险处置
B 应急响应
C 风险管理
D 风险评估

174.信息安全管理体系描述不正确的是:
A 是一个组织整体管理体系的组成部分
B 是有范围和边界的
C 是风险评估的手段
D 其基本过程应遵循 PDCA 循环

175.下面对 PDCA 模型的解释不正确的是:
A 通过规划、实施、检查和处置的工作程序不断改进对系统的管理活动
B 是一种可以应用于信息安全管理活动持续改进的有效实践方法
C 也被称为"戴明环"
D 适用于对组织整体活动的优化，不适合单个的过程以及个人

176.在 PDCA 摸型中，ACT(处置）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

177.以下对 PDCA 循环特点描述不正确的是：
A 按顺序进行，周而复始，不断循环
B 组织中的每个部分,甚至个人,均可以 PDCA 循环,大环套小环,一层一层地解决问题
C 每通过一次 PDCA 循环,都要进行总结,提出新目标,再进行第二次 PDCA 循环
D 可以由任何一个阶段开始，周而复始，不断循环

178.ISMS 过程中，实施信息安全教育应在哪个阶段进行?

A 实施和运行
B 保持和改进
C 建立
D 监视和评审

179.对"PDCA"循环的描述不正确的是:
A “PDCA”的含义是 P-计划，D-实施，C-检查，A-改进
B “PDCA”循环又叫"戴明"环
C “PDCA"循环是只能用于信息安全管理体系有效进行的工作程序
D “PDCA”循环是可用于任何一项活动有效进行的工作程序

180.下述选项中对于"风险管理"的描述不正确的是:
A 风险管理是指导和控制一个组织相关风险的协调活动，它通常包括风险评估、风险处置、风险接受和风险沟通。
B 风险管理的目的是了解风险并采取措施处置风险并将风险消除。
C 风险管理是信息安全工作的重要基础，因此信息安全风险管理必须贯穿到信息安全保障工作、信息系统的整个生命周期中。
D 在网络与信息系统规划设计阶段，应通过信息安全风险评估进一步明确安全需求和安全目标。

181.风险是需要保护的()发生损失的可能性，它是()和()综合结果。
A 资产，攻击目标，威胁事件
B 设备、威胁、漏洞
C 资产，威胁，漏洞
D 以上都不对

182.下面威胁中不属于抵赖行为的是:
A 发信者事后否认曾经发送过某条消息
B 收信者事后否认曾经接收过某条消息
C 发信者事后否认曾经发送过某条消息的内容
D 收信者接收消息后更改某部分内容

183.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

184.以下列哪种处置方法属于转移风险?
A 部署综合安全审计系统
B 对网络行为进行实时监控
C 制订完善的制度体系
D 聘用第三方专业公司提供维护外包服务

186.对操作系统打补丁和系统升级是以下哪种风险控制措施?

A 降低风险
B 规避风险
C 转移风险
D 接受风险

187.以下哪一项可认为是具有一定合理性的风险?
A 总风险
B 最小化风险
C 可接受风险
D 残余风险

188.在风险管理工作中“监控审查”的目的，一是:二是
A 保证风险管理过程的有效性，保证风险管理成本的有效性
B 保证风险管理结果的有效性，保证风险管理成本的有效性
C 保证风险管理过程的有效性，保证风险管理活动的决定得到认可
D 保证风险管理结果的有效性，保证风险管理活动的决定得到认可

189.风险管理四个步骤的正确顺序是:
A 背景建立、风险评估、风险处理、批准监督
B 背景建立、风险评估、审核批准、风险控制
C 风险评估、对象确立、审核批准、风险控制
D 风险评估、风险控制、对象确立、审核批准

190.在风险管理的过程中，"建立背景"(即"对象确立")的过程是哪四个活动?
A 风险管理准备、信息系统调查、信息系统分析、信息安全分析
B 风险管理准备、信息系统分析、信息安全分析、风险政策的制定
C 风险管理准备、风险管理政策的制定、信息系统分析、信息安全分析
D 确定对象、分析对象、审核对象、总结对象

191.下列对风险分析方法的描述正确的是:
A 定量分析比定性分析方法使用的工具更多
B 定性分析比定量分析方法使用的工具更多
C 同一组织只用使用一种方法进行评估
D 符合组织要求的风险评估方法就是最优方法

192.某公司正在进行信息安全风险评估,在决定信息资产的分类与分级时,谁负有最终责任?
A 部门经理
B 高级管理层
C 信息资产所有者
D 最终用户

193.在一个有充分控制的信息处理计算中心中，下面酬的可以自同一个人执行?
A 安全管理和变更管理
B 计算机操作和系统开发

C 系统开发和变更管理
D 系统开发和系统维护

194.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，分自己给不同人员完成
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

195.根据灾难恢复演练的深度不同，可以将演练分为三个级别，这三个级别按演练深度由低到高的排序正确的是·
A 系统级演练、业务级演练、应用级演练
B 系统级演练、应用级演练、业务级演练
C 业务级演练、应用级演练、系统级演练
D 业务级演练、系统级演练、应用级演练

196.以下哪一个是对“岗位轮换“这一人员安全管理原则的正确理解?
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

197.在构建一个单位的内部安全管理组织体系的时候，以下哪一项不是必需考虑的内容?
A 高级管理层承诺对安全工作的支持
B 要求雇员们遵从安全策略的指示
C 在第三方协议中强调安全
D 清晰地定义部门的岗位的职责

198.灾难发生后，系统和数据必须恢复到的
A 时间要求
B 时间点要求
C 数据状态
D 运行状态

199 当发现信息系统被攻击时，以下哪一项是首先应该做的?
A 切断所有可能导致入侵的通信线路
B 采取措施遏制攻击行为
C 判断哪些系统和数据遭到了破坏
D 与有关部门联系

200.应急方法学定义了安全事件处理的流程，这个流程的顺序是:
A 准备-遏制-检测-根除-恢复-跟进
B 准备-检测-遏制-恢复-根除-跟进
C 准备-检测-遏制-根除-恢复-跟进

D 准备-遏制-根除-检测-恢复-跟进

201.以下哪种情形下最适合使用同步数据备份策略?
A 对灾难的承受能力高
C 恢复时间目标(RTO)长
C 恢复点目标(RPO)短
D 恢复点目标(RPO)长

202.当备份一个应用程序系统的数据时，以下哪一项是应该首先考虑的关键性问题?
A 什么时候进行备份?
B 在哪里进行备份?
C 怎样存储备份?
D 需要各份哪些数据?

203.下面对于 SSE-CMM 保证过程的说法错误的是:
A 保证是指安全需求得到满足的可信任程度
B 信任程度来自于对安全工程过程结果质量的判断
C 自验证与证实安全的主要手段包括观察、论证、分析和测试
DPA“建立保证论据”为 PA“验证与证实安全"提供了证据支持

204.下面对能力成熟度模型解释最准确的是:
A 它认为组织的能力依赖于严格定义、管理完善、可测可控的有效业务过程
B 它通过严格考察工程成果来判断工程能力
C 它与统计过程控制理论的出发点不同，所以应用于不同领域
D 它是随着信息安全的发展而诞生的重要概念

205.SSE-CMM，即系统安全工程---能力成熟度模型,它的六个级别,其中计划和跟踪级着重于
A 规范化地裁剪组织层面的过程定义
B 项目层面定义、计划和执行问题
C 测量
D 一个组织或项目执行了包含基本实施的过程

206.信息安全工程监理工程师不需要做的工作是:
A 编写验收测试方案
B 审核验收测试方案
C 监督验收测试过程
D 审核验收测试报告

207.信息安全工程监理的作用不包括下面哪一项?
A 弥补建设单位在技术与管理上的经验不足
B 帮助承建单位攻克技术难点，顺利实施项目
C 改善建设单位与承建单位之间的交流沟通
D 通过监理控制积极促进项目保质按期完成

208.美国国防部公布的《可信计算机系统评估准则》(TCSEC)把计算机系统的安全分为个大的等级。
A3
B4
C5
D6

209.以下对确定信息系统的安全保护等级理解正确的是:
A 信息系统的安全保护等级是信息系统的客观属性
B 确定信息系统的安全保护等级时应考虑已采取或将采取的安全保护措施
C 确定信息系统的安全保护等级时应考虑风险评估的结果
D 确定信息系统的安全保护等级时应仅考虑业务信息的安全性

210.依据 GB/T24364-2009《信息安全技术信息安全应急响应计划规范》，应急响应方法论的响应过程的第二步是
A 准备
B 确认
C 遏制
D 根除

211.各国在信息安全保障组织架构有两种主要形式，一种是由一个部门集中管理国家信息安全相关工作，另一种是多个部门分别管理，同时加强协调工作。下列各国中，哪一个国家是采取多部门协调的做法:
A 德国
C 法国
C 美国
D 以上国家都不是

212.是目前国际通行的信息技术产品安全性评估标准?
ATCSEC
BITSEC
CCC
DIATF

213.下列哪项不是《信息安全等级保护管理办法》(公通字[2007]43 号)规定的内容:
A 国家信息安全等级保护坚持自主定级、自主保护的原则
B 国家指定专门部门对信息系统安全等级保护工作进行专门的监督和检查
C 跨省或全国统一联网运行的信息系统可由主管部门统一确定安全保护等级
D 涉及国家秘密的信息系统不进行分等级保护

214.以下哪一项不是我国与信息安全有关的国家法律?
A《信息安全等级保护管理办法》
B《中华人民共和国保守国家秘密法》
C《中华人民共和国刑法》

D《中华人民共和国国家安全法》

215.根据我国信息安全管理体系，党政机关信息网络的安全保卫任务有下列哪个单位负责?
A 公安机关
B 国家安全机关
C 国家保密工作部门
D 国家密码主管部门

216.下列哪个不是《商用密码管理条例》规定的内容?
A 国家密码管理委员会及其办公室(简称密码管理机构)主管全国的商用密码管理工作
B 商用密码技术属于国家秘密，国家对商用密码产品的科研、生产、销售和使用实行专控管理
C 商用密码产品由国家密码管理机构许可的单位销售
D 个人可以使用经国家密码管理机构认可之外的商用密码产品

207.以下哪些问题或概念不是公钥密码体制中经常使用到的困难问题?
A、大整数分解
B、离散对数问题
C、背包问题
D、伪随机数发生器

208.以下哪种公钥密码算法既可以用于数据加密又可以用于密钥交换?
A、DSS
B、Diffie-Hellman
C、RSA
D、AES

209.IPSec 协议中的 AH 协议不能提供下列哪一项服务?
A、数据源认证
B、数据包重放
C、访问控制
D、机密性

210.下面哪一项内容更准确地描述了网络接口层(即数据链路层)可能存在的安全攻击?
A、ARP 欺骗、分片攻击、synflood 等
B、ARP 欺骗、macfloodin，嗅探等
C、死亡之 ping、macflooding、嗅探等
D、IP 源地址欺骗、ARP 欺骗、嗅探等

211.简单包过滤防火墙主要工作在
A、链路层/网络层
B、网络层/传输层
C、应用层
D、会话层

212.下列 SQL 语句给出关系型数据库中的哪一类完整性约束条件?
CREATETABLEStudent
(idCHAR(8).
SnameCHAR(20)NOTNULL，
SageSMALLINT.
PRIMARYKEY(id)
A 实体完整性
B 二维表完整性
C 参照完整性
D 自定义完整性

213.杀毒软件报告发现病毒 Macro.Melissa,由该病毒名称可以推断出病毒类型是
A 文件型
B 引导型
C 目录型
D 宏病毒

214.下述选项中对于"风险管理"的描述正确的是:
A 安全必须是完美无缺、面面俱到的。
B 最完备的信息安全策略就是最优的风险管理对策
C 在应对信息安全风险时,要从经济、技术、管理的可行性和有效性上做出权衡和取舍.
D 防范不足就会造成损失:防范过多就可以避免损失。

215.应对信息安全风险的主要目标是什么?
A 消除可能会影响公司的每一种威胁
B 管理风险，以使由风险产生的问题降至最低限度
C 尽量多实施安全措施以消除资产暴露在其下的每一种风险
D 尽量忽略风险，不使成本过高

216 当员工或外单位的工作人员离开组织或岗位变化时，必须进行以下的管理程序除了:
A 明确此人不再具有以前的职责
B 确保归还应当归还的资产
C 确保属于以前职责的访问权限被撤销
D 安全管理员陪同此人离开工作场所

217.IATF 深度防御战略的三个层面不包括:
A.人员
B.法律
C.技术
D.运行

218.“中华人民共和国保守国家秘密法”第二章规定了国家秘密的范围和密级，国家秘密的密级分为:
A.“普密”、“商密”两个级别

B.“低级”和“高级”两个级别
C.“绝密”、“机密”、“秘密”三个级别
D.“一密”、“二密”、“三密”、“四密”四个级别

219.触犯新刑法 285 条规定的非法入侵计算机系统罪可判处_____。
A.假冒源地址或用户的地址的欺骗攻击
B.抵赖做过信息的递交行为
C.数据传输中被窃听获取
D.数据传输中被篡改或破坏

220.以下关于我国信息安全政策和法律法规的说法错误的是：
A.中办方【2003】27 号文提出“加快信息安全人员培养，增强全民信息安全意识”
B.2008 年 4 月国务院办公厅发布了《关于加强政府信息系统安全和保密管理工作的通知》
C.2007 年我国四部委联合发布了《信息安全等级保护管理办法》
D.2006 年 5 月全国人大常委会审议通过了《中国人民共和国信息安全法》

221.信息安全保障要素不包括以下哪一项？
A.技术
B.工程
C.组织
D.管理

222.以下关于信息安全保障说法中哪一项不正确？
A.信息安全保障是为了支撑业务高效稳定的运行
B.以安全促发展，在发展中求安全
C.信息安全保障不是持续性开展的活动
D.信息安全保障的实现，需要将信息安全技术与管理相结合

223.信息安全保障是一种立体保障，在运行时的安全工作不包括：
A.安全评估
B.产品选购
C.备份与灾难恢复
D.监控

224.以下对信息安全风险管理理解最准确的说法是：
A.了解风险
B.转移风险
C.了解风险并控制风险
D.了解风险并转移风险

225.“进不来”“拿不走”“看不懂”“改不了”“走不脱”是网络信息安全建设的目的。其中，“看不懂”是指下面哪种安全服务：
A.数据加密
B.身份认证

C.数据完整性
D.访问控制
226.拒绝服务攻击损害了信息系统的哪一项性能？
A.完整性
B.可用性
C.保密性
D.可靠性

227.VPN 系统主要用于_____
A.进行用户身份的鉴别
B.进行用户行为的审计
C.建立安全的网络通信
D.对网络边界进行访问控制

228.下列哪些描述同 SSL 相关？
A.公钥使用户可以交换会话密钥、解密会话密钥并验证数字签名的真实性
B.公钥使用户可以交换会话密钥、验证数字签名的真实性以及加密数据
C.私钥使用户可以创建数字签名、验证数字签名的真实性并交换会话密钥
D.私钥使用户可以创建数字签名、加密数据和解密会话密钥

229.VPN 技术无法实现以下哪个服务？
A.身份验证
B.传输加密
C.完整性校验
D.可用性校验

230.SSL 协议比 IPSEC 协议的优势在于：
A.实现简单、易于配置
B.能有效的工作在网络层
C.能支撑更多的应用层协议
D.能实现更高强度的加密

231.Windows 操作系统的注册表运行命令是：
A.Regsvr32
B.Regedit
C.Regedit.msc
D.Regedit.mmc

232.视窗操作系统（Windows）从哪个版本开始引入安全中心的概念？
A.WinNTSP6
B.Win2000SP4
C.WinXPSP2
D.Win2003SP1

233.在 linux 系统中拥有最高级别权限的用户是：
A.root
B.administrator
C.mail
D.nobody

234.下面对于“电子邮件炸弹”的解释最准确的是：
A.邮件正文中包含的恶意网站链接
B.邮件附件中具有强破坏性的病毒
C.社会工程的一种方式，具有恐吓内容的邮件
D.在短时间内发送大量邮件的软件，可以造成目标邮箱爆满

235.在应用层协议中，_____可使用传输层的 TCP 协议，又可用 UDP 协议。
A.SMTP
B.DNS
C.HTTP
D.FTP

236.以下哪一项是伪装成所有程序的恶意软件？
A.计算机病毒
B.特洛伊木马
C.逻辑程序
D.蠕虫程序

237.下列哪个是蠕虫的特性？
A.不感染、依附性
B.不感染、独立性
C.可感染、依附性
D.可感染、独立性

238.下列哪种恶意代码不具备“不感染、依附性”的特点？
A.后门
B.陷门
C.木马
D.蠕虫

239.下面哪类设备常用于识别系统中存在的脆弱性？
A.防火墙
B.IDS
C.漏洞扫描器
D.UTM

240.某种防火墙的缺点是没有办法从非常细微之处来分析数据包，但它的优点是非常快，这种防火墙是以下的哪一种？

A.电路级网关
B.应用级网关
C.会话层防火墙
D.包过滤防火墙

241.下面哪一种是社会工程?
A.缓冲器溢出
B.SQL 注入攻击
C.电话联系组织机构的接线员询问用户名和口令
D.利用 PKI/CA 构建可信网络

242.以下哪一项不是 IDS 可以解决的问题?
A.弥补网络协议的弱点
B.识别和报告对数据文件的改动
C.统计分析系统中异常活动模式
D.提升系统监控能力

243.下列关于防火墙功能的说法最准确的是:
A.访问控制
B.内容控制
C.数据加密
D.查杀病毒

244.一台需要与互联网通信的 WEB 服务器放在以下哪个位置最安全?
A.在 DMZ 区
B.在内网中
C.和防火墙在同一台计算机上
D.在互联网防火墙外

245.路由器在两个网段之间转发数据包时，读取其中的（）地址来确定下一跳的转发路径。
A.IP
B.MAC
C.源
D.ARP

246.在包过滤型防火墙中，定义数据包过滤规则的是:
A.路由表
B.ARP
C.NAT
D.ACL

247.包过滤型防火墙对数据包的检查内容一般不包括_____。
A.源地址
B.目的地址

C.协议
D.有效载荷

248.NAT 技术不能实现以下哪个功能？
A.对应用层协议进行代理
B.隐藏内部地址
C.增加私有组织的地址空间
D.解决 IP 地址不足问题

249.某单位想用防火墙对 telnet 协议的命令进行限制，应选在什么类型的防火墙？
A.包过滤技术
B.应用代理技术
C.状态检测技术
D.NAT 技术

250.某单位通过防火墙进行互联网接入，外网口地址为 202.101.1.1，内网口地址为 192.168.1.1，这种情况下防火墙工作模式为：
A.透明模式
B.路由模式
C.代理模式
D.以上都不对

251.以下哪个是防火墙可以实现的效果？
A.有效解决对合法服务的攻击
B.有效解决来自内部的攻击行为
C.有效解决来自互联网对内网的攻击行为
D.有效解决针对应用层的攻击

252.某单位采购主机入侵检测，用户提出了相关的要求，其中哪条是主机入侵检测无法实现的？
A.精确地判断攻击行为是否成功
B.监控主机上特定用户活动、系统运行情况
C.监测到针对其他服务器的攻击行为
D.监测主机上的日志信息

253.某单位采购主机入侵检测，用户提出了相关的要求，其中哪条要求是错误的？
A.实时分析网络数据，检测网络系统的非法行为
B.不占用其他计算机系统的任何资源
C.不会增加网络中主机的负担
D.可以检测加密通道中传输的数据

254.以下哪个入侵检测技术能检测到未知的攻击行为？
A.基于误用的检测技术
B.基于异常的检测技术
C.基于日志分析的技术

D.基于漏洞机理研究的技术

255.某单位将对外提供服务的服务器部署在防火墙 DMZ 区，为了检测到该区域中的服务器受到的攻击行为，应将防火墙探头接口镜像那个位置的流量？
A.内网核心交换机
B.防火墙互联网接口
C.防火墙 DMZ 区接口
D.以上都可以

256.关于数据库注入攻击的说法错误的是：
A.它的主要原因是程序对用户的输入缺乏过滤
B.一般情况下防火墙对它无法防范
C.对它进行防范时要关注操作系统的版本和安全补丁
D.注入成功后可以获取部分权限

257.监听网络流量获取密码，之后使用这个密码试图完成未经授权访问的攻击方式被称为：
A.穷举攻击
B.字典攻击
C.社会工程攻击
D.重放攻击

258.“TCPSYNPlooding”建立大量处于半连接状态的 TCP 连接，其攻击目标是网络的_____。
A.保密性
B.完整性
C.真实性
D.可用性

259.ICMP 协议有多种控制报文，当网络出现拥塞时候，路由器发出_____报文。
A.路由重定向
B.目标不可达
C.源抑制
D.子网掩码请求

260.通过反复尝试向系统提交用户名和密码以发现正确的用户密码的攻击方式称为：
A.账户信息收集
B.密码分析
C.密码嗅探
D.密码暴力破解

261.在 Windows 文件系统中，_____支持文件加密。
A.FAT16
B.NTFS
C.FAT32
D.EXT3

262.下列保护系统账户安全的措施中，哪个措施对解决口令暴力破解无帮助？
A.设置系统的账户锁定策略，在用户登录输入错误次数达到一定数量时对账户进行锁定
B.更改系统内置管理员的用户名
C.给管理员账户一个安全的口令
D.使用屏幕保护并设置返回时需要提供口令

263.关闭系统中不需要的服务主要目的是：
A.避免由于服务自身的不稳定影响系统的安全
B.避免攻击者利用服务实现非法操作从而危害系统安全
C.避免服务由于自动运行消耗大量系统资源从而影响效率
D.以上都是

264.某系统被攻击者入侵，初步怀疑为管理员存在弱口令，攻击者从远程终端以管理员身份登录进行系统进行了相应的破坏，验证此事应查看：
A.系统日志
B.应用程序日志
C.安全日志
D.IIS 日志

265.U 盘病毒的传播是借助 Windows 系统的什么功能实现的？
A.自动播放
B.自动补丁更新
C.服务自启动
D.系统开发漏洞

266.保护数据安全包括保密性、完整性和可用性，对于数据的可用性解决方法最有效的是：
A.加密
B.备份
C.安全删除
D.以上都是

267.在 Windows 系统中，管理权限最高的组是：
A.everyone
B.administrators
C.powerusers
D.users

268.Windows 系统下，可通过运行_____命令打开 Windows 管理控制台。
A.regedit
B.cmd
C.mmc
D.mfc

269.信息安全风险的三要素是指：
A.资产/威胁/脆弱性
B.资产/使命/威胁
C.使命/威胁/脆弱性
D.威胁/脆弱性/使命

270.以下哪一项是已经被确认了的具有一定合理性的风险？
A.总风险
B.最小化风险
C.可接受风险
D.残余风险

271.统计数据指出，对大多数计算机系统来说，最大的威胁是：
A.本单位的雇员
B.黑客和商业间谍
C.未受培训的系统用户
D.技术产品和服务供应商

272.下列安全协议中，_____可用于安全电子邮件加密。
A.PGP
B.SET
C.SSL
D.TLS

273.HTTPS 采用_____协议实现安全网站访问。
A.SSL
B.IPSec
C.PGP
D.SET

274.信息安全等级保护制度是国家保障和促进信息化建设健康发展的一项基本制度，信息系统安全保护等级分为：
A.3 级
B.4 级
C.5 级
D.6 级

275.下列哪项 ISO27000 系列是关于 ISMS 要求的？
A.ISO27001
B.ISO27002
C.ISO27003
D.ISO27004

276.下列哪项 ISO27000 系列是关于 ISMS 要求的？

A.ISO27001
B.ISO27002
C.ISO27003
D.ISO27004

277.以下对于信息安全管理体系说法不正确的是：
A.P（Process）：处理
B.D（Do）：实施
C.C（Check）：检查
D.A（Action）：行动

278.风险管理中使用的控制措施，不包括以下哪种类型？
A.预防性控制措施
B.管理性控制措施
C.检查性控制措施
D.纠正性控制措施

279.风险管理中的控制措施不包括以下哪一方面？
A.行政
B.道德
C.技术
D.管理

280.风险评估不包括以下哪个活动？
A.中断引入风险的活动
B.识别资产
C.识别威胁
D.分析风险

281.在信息安全风险管理工作证，识别风险时主要重点考虑的要素应包括：
A.资产及其价值、威胁、脆弱性、现有的和计划的控制措施
B.资产及其价值、系统的漏洞、脆弱性、现有的和计划的控制措施
C.完整性、可用性、机密性、不可抵赖性
D.减低风险、转嫁风险、规避风险、接受风险

282.以下哪一项不是信息安全风险分析过程中所要完成的工作：
A.识别用户
B.识别脆弱性
C.评估资产价值
D.计算机安全事件发生的可能性

283.机构应该把信息系统安全看作：
A.业务中心
B.风险中心

C.业务促进因素
D.业务抑制因素
284.以下关于 ISO/IEC27001 所应用的过程方法主要特点说法错误的是：
A.理解组织的信息安全要求和建立信息安全方针与目标的标准
B.从组织整体业务风险的角度管理组织的信息安全风险
C.监视和评审 ISMS 的执行情况和有效性
D.基于主观测量的持续改进

285.在检查岗位职责时什么是最重要的评估标准？
A.工作职能中所有要做的工作和需要的培训都有详细的定义
B.职责清晰，每个人都清楚自己在组织中的角色
C.强制休假和岗位轮换被执行
D.绩效得到监控和提升是基于清晰定义的目标

286.在信息安全管理中进行_____，可以有效解决人员安全意识薄弱问题。
A.内容监控
B.安全教育和培训
C.责任追查和惩处
D.访问控制

287.以下哪一项最能体现 27002 管理控制措施中预防控制措施的目的？
A.减少威胁的可能性
B.保护企业的弱点区域
C.减少灾难发生的可能性
D.防御风险的发生并降低其影响

288.关于外包的论述不正确的是：
A.企业经营管理中的诸多操作成服务都可以外包
B.通过业务外包，企业也把相应的风险承担者转移给了外包商，企业从此不必对外包业务负任何直接或间接的责任
C.虽然业务可以外包，但是对与外包业务的可能的不良后果，企业仍然承担责任
D.过多的外包业务可能产生额外的操作风险或其他隐患

289.关于 SSE-CMM 的描述错误的是：
A.1993 年 4 月美国国家安全局资助，有安全工业界、美国国防部办公室和加拿大通信安全机构共同组成 SSE-CMM 项目组
B.SSE-CMM 的能力级别分为 6 个级别
C.SSE-CMM 将安全工程过程划分为三类：风险、工程和保证
D.SSE 的最高能力级别是量化控制

290.以下对 SSE-CMM 描述正确的是：
A.它是指信息安全工程能力成熟模型
B.它是指系统安全技术能力成熟的模型
C.它是指系统安全工程能力成熟的模型

D.它是指信息安全技术能力成熟的模型

291.下面对 SSE-CMM 保证过程的说法错误的是：
A.保证是指安全需求得到满足的可信任程度
B.信任程度来自于对安全工程过程结果质量的判断
C.自验证与证实安全的主要手段包括观察、论证、分析和测试
D.PA“建立保证论据”为 PA“验证与证实安全”提供了证据支持

292.下面哪一项为系统安全工程能力成熟度模型提供了评估方法：
A.ISSE
B.SSAM
C.SSR
D.GEM

293.按照 SSE-CMM，能力级别第三级是指：
A.定量控制
B.计划和跟踪
C.持续改进
D.充分定义

294.下列哪项不是 SSE-CMM 模型中工程过程的过程区别？
A.明确安全需求
B.评估影响
C.提供安全输入
D.协调安全

295.下列哪项不是 SSE-CMM 中规定的系统安全工程过程类：
A.工程
B.组织
C.项目
D.资产

296.IT 工程建设与 IT 安全工程建设脱节是众多安全风险涌现的根源，同时安全风险也越来越多地体现在应用层，因此迫切需要加强对开发阶段的安全考虑，特别是要加强对数据安全性的考虑，以下哪项工作是在 IT 项目的开发阶段不需要重点考虑的安全因素：
A.操作系统的安全加固
B.输入数据的校验
C.数据处理过程控制
D.输出数据的验证

297.在 IT 项目管理中为了保证系统的安全性，应当充分考虑对数据的正确处理，以下哪一项不是对数据输入进行校验可以实现的安全目标：
A.防止出现数据范围以外的值
B.防止出现错误的数据处理顺序

C.防止缓冲区溢出攻击
D.防止代码注入攻击

298.以下对信息安全问题产生的根源描述最准确的是：
A.信息安全问题是由于信息技术的不断发展造成的
B.信息安全问题是由于黑客组织和犯罪集团追求名和利造成的
C.信息安全问题是由于信息系统的设计和开发过程中的疏忽造成的
D.信息安全问题产生的内因是信息系统的复杂性，外因是对手的威胁与破坏

299.PPDR 模型不包括：
A.策略
B.检测
C.响应
D.加密

300.关于信息安全策略的说法中，下面说法正确的是：
A．信息安全策略的制定是以信息系统的规模为基础
B．信息安全策略的制定是以信息系统的网络拓扑结构为基础
C．信息安全策略是以信息系统风险管理为基础
D．在信息系统尚未建设完成之前，无法确定信息安全策略

301.下面对 ISO27001 的说法最准确的是：
A．该标准的题目是信息安全管理体系实施指南
B．该标准为度量信息安全管理体系的开发和实施过程提供的一套标准
C．该标准提供了一组信息安全管理相关的控制措施和最佳实践
D．该标准为建立、实施、运行、监控、审核、维护和改进信息安全管理体系提供了一个模型

302.根据《信息系统安全等级保护定级指南》，信息系统的安全保护等级由哪两个定级要素决定？
A.威胁、脆弱性
B.系统价值、风险
C.信息安全、系统服务安全
D.受侵害的客体、对客体造成侵害的程度业务

303．VPN 系统主要用来_____
A．进行用户身份的鉴别
B．进行用户行为的审计
C．建立安全的网络通信
D．对网络边界进行访问控制

304．组成 IPSec 的主要安全协议不包括以下哪一项？
A．ESP
B．DSS
C．IKE
D．AH

305．以下哪一项是伪装成有用程序的恶意软件？
A．计算机病毒
B．特洛伊木马
C．逻辑炸弹
D．蠕虫程序

306．下列哪个是蠕虫的特征？
A．不感染、依附性
B．不感染、独立性
C．可感染、依附性
D．可感染、独立性

307．所谓网络内的机器遵循同一“协议”就是指：
A．采用某一套通信规则或标准
B．采用同一种操作系统
C．用同一种电缆互连
D．用同一种程序设计语言

308．_____设备可以隔离 ARP 广播帧
A．路由器
B．网桥
C．以太网交换机
D．集线器

309．下面哪类设备常用于识系统中存在的脆弱性？
A．防火墙
B．IDS
C．漏洞扫描器
D．UTM

310．从分析式上入侵检测技术可以分为：
A．基于标志检测技术、基于状态检测技术
B．基于异常检测技术、基于流量检测技术
C．基于误用检测技术、基于异常检测技术
D．基于标志检测技术、基于误用检测技术

311．做渗透测试的第一步是：
A．信息收集
B．漏洞分析与目标选定
C．拒绝服务攻击
D．尝试漏洞利用

312．下面哪一项是社会工程？

A．缓冲器溢出
B．SQL 注入攻击
C．电话联系组织机构的接线员询问用户名和口令
D．利用 PK/CA 构建可信网络

313.在 window 系统中用于显示本机各网络端口详细情况的命令是:
A．netshow
B．netstat
C．ipconfig
D．netview

314．在 WindowsXP 中用事件查看器查看日志文件，可看到的日志包括?
A．用户访问日志、安全性日志、系统日志和 IE 日志
B．应用程序日志、安全性日志、系统日志和 IE 日志
C．网络攻击日志、安全性日志、记账日志和 IE 日志
D．网络链接日志、安全性日志、服务日志和 IE 日志

315．下面哪个不是 ISO27000 系列包含的标准?
A.《信息安全管理体系要求》
B.《信息安全风险管理》
C.《信息安全度量》
D.《信息安全评估规范》

316．以下对信息安全管理体系说法不正确的是：
A．基于国际标准 ISO/IEC27000
B．它是综合信息安全管理和技术手段，保障组织信息安全的一种方法
C．它是管理体系家族的一个成员
D．基于国际标准 ISO/IEC27001

317．以下对 PDCA 循环解释不正确的是:
A．P（Process）：处理
B．D（Do）：实施
C．C（Check）：检查
D．A（Action）：行动

318．在 SSE-CMM 中对工程过程能力的评价分为三个层次，由宏观到微观依次是:
A．能力级别-公共特征(CF)-通用实践(GP)
B．能力级别-通用实践-(GP)-公共特征(CF)
C．通用实践-(GP)-能力级别-公共特征(CF)
D．公共特征(CF)-能力级别-通用实践-(CP)

319．根据 SSE-CMM，安全工程过程能力由低到高划分为:
A．未实施、基本实施、计划跟踪、充分定义、量化控制和持续改进等 6 个级别
B．基本实施、计划跟踪、充分定义、量化控制和持续改进等 5 个级别

C．基本实施、计划跟踪、量化控制、充分定义和持续改进等 5 个级别
D．未实施、基本实施、计划跟踪、充分定义 4 个级别

320．下列哪项不是 SSE-CMM 模型中工程过程的过程区域？
A．明确安全需求
B．评估影响
C．提供安全输入
D．协调安全

321．系统安全工程不包含以下哪个过程类:
A．工程过程类
B．组织过程类
C．管理过程类
D．项目过程类

322．ISSE(信息系统安全工程)是美国发布的 IATF3.0 版本中提出的设计和实施信息系统_____。
A．安全工程方法
B．安全工程框架
C．安全工程体系结构
D．安全工程标准

323、不同信息安全发展阶段，信息安全具有不同的的特征，在信息安全保障阶段信息安全的基本特征不包括：
A 具有高度复杂性和不能控制的特点
B 具有保护对象全生命周期安全要求的特征
C 具有多层次和多角度的体系化防御要求的特征
D 具有动态发展变化的特征

324、信息安全工作具有投资收益的要求，以下关于信息安全与业务发展的关系说法最准确的是：
A 信息安全的投入很容易测算其产生收益的
B 信息安全为业务发展提供基础安全保障
C 信息安全与网络信息系统有着密切联系
D 信息安全的投入是不能测算其产生收益的

325、PDR 模型和 P2DR 模型采用了动态循环的机制实现系统保护、检测和响应。这种模型的特点理解错误的是：
A、模型已入了动态时间基线，符合信息安全发展理念
B、模型强调持续的保护和响应，符合相对安全理念
C、模型是基于人为的管理和控制而运行的
D、模型引入了多层防御机制，符合安全的“木桶原理”

326、CC 标准是目前国际通行的信息安全技术产品安全性评价规范，关于其先进性说法错误的是：

A、它基于保护轮廓和安全目标提出安全需求，具有灵活性和合理性
B、它基于功能要求和保证要求进行安全评估，能够实现分级评估目标
C、它不仅考虑了保密性评估要求，还考虑了完整性和可用性多方面安全要求
D、它划分为 A、B、C、D 四个等级，实现分级别的安全性评测

327、下列关于 kerckhofff 准则的说法正确的是：
A、保持算法的秘密性比保持密钥的秘密性要困难的多
B、密钥一旦泄漏，也可以方便的更换
C、在一个密码系统中，密码算法是可以公开的，密钥应保证安全
D、公开的算法能够经过更严格的安全性分析

328、信息发送者使用_____进行数字签名。
A、己方的私钥
B、己方的公钥
C、对方的私钥
D、对方的公钥

329、以下哪一项不是 PKI/CA 要解决的问题：
A、可用性、身份鉴别
B、可用性、授权与访问控制
C、完整性、授权与访问控制
D、完整性、身份鉴别

330 、ISO7498-2 开放系统安全互联体系架构模型描述了信息系统安全架构的层面、实现机制和安全服务，以下哪一项不是该模型涉及的安全机制
A、鉴别
B、数字签名
C、访问控制
D、路由控制

331、操作系统安全的基础是建立在：
A、安全安装
B、安全配置
C、安全管理
D、以上都对

332、ISO27002 的内容结构按照_____进行组织
A、管理制度
B、管理原则
C、管理框架
D、管理类-----控制目标----------控制措施

333、ISO27002 中描述的 11 个信息安全管理的控制领域不包括：
A、信息安全组织
B、资产管理
C、内容安全
D、人力资源安全

334、全面构建我国信息安全人才体系是国家政策、组织机构信息安全保障建设和信息安全有关人员自身职业发展三方面的共同要求，“加快信息安全人才培养，增强全民信息安全意识”的指导精神，是以下哪一个国家政策文件提出的？
A、《国家信息化领导小组关于加强信息安全保障工作的意见》
B、《信息安全等级保护管理办法》
C、中华人民共和国计算机信息系统安全保护条例》
D、《关于加强政府信息系统安全和保密管理工作的通知》

335、我国信息系统安全等级保护工作环节依次是：
A、定级-检查-建设整改-等级测评-备案
B、等级测评-建设整改-监督检查
C、定级-备案-建设整改-等级测评-监督检查
B、定级-等级测评-备案-建设整改-监督检查

336、对信息技术保障框架的内涵和特点（IATF）理解不正确的是
A、基于 PDCA 思想构建攻防一体化安全体系
B、对信息系统进行多层保护
C、IATF 描述了保护领域的安全需求和相应的可选择措施
D、它体现了分层、深度、强健性的防御特点

337、以下关于 CC 标准说法错误的是：
A、通过评估有助于增强用户对于 IT 产品的安全信息
B、促进 IT 产品和系统安全性
C、清楚重复的评估
D、详细描述了安全评估方法学

338、以下那种信息安全工作实践应用了信息安全保障的核心原理和思想？
A、以 ISMS 运行为核心，采用技术和管理手段对建设好的系统进行维护
B、以 IATF 为基础，涉及包括防毒、入侵检测、加密、审计在内的安全防护体系
C、以 CIA 为核心，对计算机网络进行安全加固、检测和评估
D、在系统生命周期内，以人为本，按照技管并重的原则，通过安全工程过程来构建安全体系

339、关于信息保障技术框架（IATF），下列说法错误的是：
A、IATF 签掉深度防御，关注本地计算环境、区域边界、网络和基础设施、支撑性基础设施等多个领域的安全保障
B、IATF 强调深度防御，即对信息系统采用多层防护，实现组织的业务安全运作
C、IATF 强调从技术、管理和人等多个角度来保障信息系统的安全
D、IATF 强调的是以安全监测、漏洞监测和自适应填充“安全间隙”为循环来提高网络安全

340、加密和解密是对数据进行的某种交换，加密和解密的过程都是在（）的控制下进行的
a、明文　b、密文　c、信息　d、密钥

341、数字签名技术室公开密钥算法的一个典型应用，在接收端，采用（）对信息进行验证
A、发送者的公钥
B、发送者的密钥
C、接收者的公钥
D、接收者的密钥

342、关于 PKI/CA 证书，下面那一种说法是错误的？
A、证书上具有证书授权中心的数字签名
B、证书上列有证书拥有者的基本信息
C、证书上列有证书拥有者的公开密钥
D、证书上列有证书拥有者的秘密密钥

343、SSL 提供那些协议上的数据安全：
A、HTTP，FTP 和 TCP/IP
B、SKIP，SNMP 和 IP
C、UDP，VPN 和 SONET
D、PPTP,DMI 和 RC4

344、以下哪种无线加密标准中那一项的安全性最弱？
A、wep　B、wpa　C、wpa2　D、wapi

345、TCP/IP 中那个协议是用来报告错误并对消息进行控制
A、ICMP　B、IGMP　C、ARP　D、SNMP

346、防火墙中网络地址转换（NAT）的主要作用是：
A、提供代理服务　B、隐藏内部网络地址
C、进行入侵检测　D、防止病毒入侵

347、国际标准化组织 ISO 下属 208 个技术委员会（TCs），531 个分技术委员会（SC）及其下设 2378 各工作组（WGs），其中负责信息安全技术标准化的组织是：
A、ISO/IEC　B、ISO/IEC JTC 1
C、ISO/IEC JTC 1/SC 27　D、ISO/IEC JTC 1/SC 37

348、以下关于 TCSEC 的说法正确的是：
A、TCSEC 对安全功能和安全保证进行了明确的区分
B、TCSEC 为评估操作系统的可信赖程度提供了一套方法
C、TCSEC 没有包括对网络和通信的安全性进行评估内容
D、数据库系统的安全性评估不在 TCSEC 的内容中

349、下面对于保护轮廓（PP）的说法最准确的是
A、对系统防护强度的描述
B、对评估对象系统进行规范化的描述
C、对一类 TOE 的安全需求，进行与技术实现无关的描述
D、由一系列保证组件构成的包，可以代表预先定义的保证尺度

350、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　　B、BS7799-2
C、ITSEC　　D、CC