信息安全专业人员知识测试试题 （一）

1. 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
解释：GB/T 20274 信息系统保障评估框架从管理、技术、工程和总体方面进行评估。

2. *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，保证已经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
解释：A 为可用性，B 为完整性，C 是抗抵赖，D 是保密性。冲正是完整性纠正措施，是 Clark-Wilson 模型的应用，解决数据变化过程的完整性。

3. **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
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
解释：美国已经设立中央政府级的专门机构。

4. 与 PDR 模型相比，P2DR（PPDR）模型多了哪一个环节?
A. 防护 B. 检测 C. 反应 D. 策略
解释：PPDR 是指策略、保护、检测和反应（或响应）。PPDR 比 PDR 多策略。

5. *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(Agreeto)、现实(Realistic)、有一定的时限(Timeoriented)
解释：据项目进度不能随机确定，需要根据项目预算、特性、质量等要求进行确定。

6. 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 Cyber security 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
解释：CNCI 第一个防线针对漏洞进行风险控制，第二个防线针对威胁进行风险控制，总体的目标是降低网络风险。B、C、D 答案均无法从题干反应。

7. 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”。
解释：D 的正确描述是从内而外，自上而下，从端到边界的防护能力。

8. 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
解释：题干为网银系统对用户的鉴别。

9. 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
解释：题干中使用到了私钥解密，私钥是公钥密码体制中用户持有的密钥，相对于公钥而言，则为非对称密码体制，非对称密码体制又称为公钥密码体制。

10. 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
解释：实体所有鉴别包括身份证、IC 卡、钥匙、USB-Key 等。

11. 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
解释：题目中安全登录会涉及到账号密码为实体所知，智能卡和短信是实体所有。

12. 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
解释：渗透测试是模拟攻击的黑盒测试，有利于发现系统明显的问题。

13. 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
解释：个人隐私包括但不限于用户名密码、位置、行为习惯等信息。

14. 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．软件上线前对软件全面安全性测试，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
解释：软件的安全测试**根据实际情况进行测试措施的选择和组合**。

15. 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
解释：L2F、PPTP、L2TP 均为二层隧道协议。

16. 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)
解释：定义主体访问客体的权限叫作 CL。定义客体被主体访问的权限叫 ACL。

---

17. 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
解释：RBAC1 模型能实现多级安全中的访问控制。

18. 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)
解释：TACACS+是 AAA 权限控制系统，不属于 VPN。

19. 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
解释：A 错误，因为使用对称密码；B 错误，因为密钥分发中心不包括客户机；D 错误，因为协议需要时钟同步。三个步骤：1）身份认证后获得票据许可票据；2）获得服务许可票据；3）获得服务。

20. 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
解释：令牌是基于实体所有的鉴别方式。

21. 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
解释：数字签名可以提供抗抵赖、鉴别和完整性。

22. 某公司已有漏洞扫描和入侵检测系统(Intrusion 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
解释：在技术条件允许情况下，可以实现 IDS 和 FW 的联动。

23. 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
解释：网络层和应用层可以提供保密性、身份鉴别、完整性、抗抵赖、访问控制服务。

24. 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哪项原则
A.最小权限 B.权限分离 C．不信任 D．纵深防御
解释：权限分离是将一个较大的权限分离为多个子权限组合操作来实现。

25. 以下关于互联网协议安全(Internet Protocol Security，IPSec)协议说法错误的是：
A．在传送模式中，保护的是 IP 负载。
B．验证头协议(Authentication Header，AH)和 IP 封装安全载荷协议(Encapsulating Security Payload，ESP)都能以传输模式和隧道模式工作。
C．在隧道模式中，保护的是整个互联网协议 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。
解释：IPSEC 可以提供身份鉴别、保密性、完整性、抗抵赖、访问控制服务。

26. 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
解释：A 属于可用性；B 保密性；C 属于完整性。

27. 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
解释：SHA 不提供加密，SHA 是摘要算法提供数据完整性校验。

28. 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
解释：IPS 在串联情况下，会影响网络性能。

29. 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问题，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
解释：NTFS 不能兼容 EXT 文件系统。

30. 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. 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
解释：在多重备份存储情况下，可以防护日志被篡改的攻击（前提非实时同步）。

31. 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
解释：一个用户可以属于多个组。

32. 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
解释：操作系统和应用安全装应分开不同磁盘部署。

33. 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
解释：数据粒度越细则授权策略越灵活便利。

34. 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
解释：漏洞是人为故意或非故意引入的弱点。

35. 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
解释：账号锁定是为了解决暴力破解攻击的。

36. 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 C. ARP 缓存是动态的，可被改写
B. 为提高效率，ARP 信息在系统中会缓存 D. ARP 协议是用于寻址的一个重要协议
解释：D 不是导致欺骗的根源。

37. 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
解释：D 属于社会工程学攻击。

38. 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
解释：设计阶段是发现和改正问题的最佳阶段。

39. 在软件保障成熟度模型(Software Assurance Maturity Mode，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
解释：SAMM 模型四个部分是治理、构造、验证和部署。

40. 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。
解释：SSE-CMM 是面向工程过程质量控制的一套方法,CC 标准面向开发、评估、交付的标准。

41. 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
解释：A 错误，BP 是基于最佳的工程过程实践；B 错误，BP 是经过测试的；D 错误，一项 BP 和其他的 BP 是不重复。

42. 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 C. 是否建立了具有自适应能力的信息安全模型
B. 是否可以抵抗大部分风险 D. 是否已经将风险控制在可接受的范围内
解释：判断风险控制的标准是风险是否控制在接受范围内。

43. 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
解释：信息安全问题是多方面存在的，不能认为主要为技术问题，同时技术漏洞不是犯罪的根源所在。

44. 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
解释：计算公式为 100 万*24%*（3/8）=9 万

45. 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
解释：电子签名不可以与认证服务提供者共有。

46. 风险管理的监控与审查不包含：
A．过程质量管理 C．跟踪系统自身或所处环境的变化
B．成本效益管理 D．协调内外部组织机构风险管理活动
解释：D 答案属于沟通咨询工作，ABC 属于风险管理的监控审查工作。风险管理过程包括背景建立、风险评估、风险处理、批准监督，以及沟通咨询和监控审查。

47. 信息安全等级保护要求中，第三级适用的正确的是：
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般损害
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严重损害
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
解释：定级原理 122-234-345，题目中 B 为等级保护三级，该考点为等级保护定级指南。
A 一级，B 三级，C 四级，D 五级。

48. 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 C．记录并分析用户和管理员操作日志
B．记录并分析系统错误日志 D．启用时钟同步
解释：A 属于防护措施；BCD 属于检测措施，可以用来检测未经授权的信息处理活动。

49. 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
解释：略

50. 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
解释：安全事件无法杜绝。

51. 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，因为预防控制功能已经足够
解释：略

52. 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
解释：D 描述的是信息安全保障工作目标；ABC 描述的是信息安全保障的原则。

53. 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
解释：安全措施投入应越早则成本越低，C 答案则成本会上升。

54. 《信息安全技术 信息安全风险评估规范》（GB／T 20984-2007）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
解释：来源于《信息安全技术 信息安全风险评估规范》（GB／T 20984-2007），原文描述 D 为“是一种较全面的风险评估”。

55. 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，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
解释：B 错误，应该是抽样评估；C 错误，应该其描述的是差距分析；D 错误，应该是威胁包括人为威胁和环境威胁。

56. 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
解释：安全策略是宏观的原则性要求，不包括具体的架构、参数和实施手段。

57. 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
解释：信息安全风险评估应以自评估（自查）为主。

58. 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
解释：通常由管理层提供各种信息安全工作必须的资源。

59. 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
解释：答案为 B。

60. 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. Ia，Va 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
解释：Ia 资产 A 的价值；Va 是资产 A 的脆弱性严重程度。

61. 以下哪一项在防止数据介质被滥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
解释：快速格式化删除存储介质中的保密文件不能防止信息泄露。

62. 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
解释：由于备份会造成个人稳私和其它敏感信息的扩散。

63. 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
解释：日志只有授权用户可以读取。

64. 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)
解释：应急响应的六个阶段是准备、检测、遏制、根除、恢复、跟踪总结。

65. 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
解释：监理模型组成包括监理咨询支撑要素、监理咨询阶段过程、控制和管理手段。

66. 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
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
解释：A 错误，因为差分备份是上次全备后的更新数据；增量备份是任何上一次备份后的更新数据。全备份周期最长、次之差分备份，更新周期最短是增量备份。B 错误，我国灾备能力级别一共分为 6 级。D 是明显的错误。

67. 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
解释：ABC 其均属于项目管理文档。需求说明书、设计说明书、测试方案、测试用例等属于开发类文档。

68. 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
解释：监理从项目招标开始到项目的验收结束，在投资计划阶段没有监理。

69. 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，数据集中，便于对数据进行管理和备份*
解释：NAS 优点数据集中、节约空间，缺点是占用网络带宽、存储中心存在单点故障。
DAS 优点数据分散、风险分散，缺点是存储空间利用率低、不便于统一管理。SAN 基于 NAS 的进一步实现，基于高速网络、多备份中心来进行实现。

70. 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
解释：答案为 A。

71. 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
解释：答案为 D，备份中心的综合风险小于主中心。

72. 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
解释：根据 BCM 的分析过程顺序为 A。

73. 有关系统安全工程-能力成熟度模型(SSE-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
解释：SSE-CMM 是系统工程，不可以独立实施。

74. 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
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
解释：信息系统安全保障要素为技术工程管理和人员四个领域。信息系统安全保障的安全特征是完整、保密和可用性。

75. 在使用系统安全工程-能力成熟度模型(SSECMM)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．测量单位是通用实践(Generic Practices，GP)
C．测量单位是过程区域(Process Areas，PA)
D．测量单位是公共特征(Common Features，CF)
解释：公共特征是衡量能力的标志。

76. 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／T20274．1-2006)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
解释：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需要投入。

77. 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
解释：D 属于项目的验收阶段，不属于 IT 项目的立项阶段，题干属于立项阶段。

78. 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各个可能位置实现所有信息安全保障机制
解释：IATF 是在网络的各位置实现所需的安全机制。

79. 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
解释：C 是渗透测试的优点。

80. 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
C.软件安全测试关注的是软件的功能
B.FUZZ 模糊测试是经常采用的安全测试方法之一
D.软件安全测试可以发现软件中产生的所有安全问题
解释：B 是正确答案。

81. 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
C.信息系统生命周期的过程安全问题
B.信息系统组成部门的组件安全问题
D.信息系统运行维护的安全管理问题
解释：正确的答案为 C。

82. 有关系统安全工程-能力成熟度模型（SSE-CMM)中基本实施（Base Practice）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
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
D.BP 不是过程区域（Process Areas，PA ）的强制项
解释：BP 属于安全工程的最小单元，其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；是根据广泛的现有资料，实施和专家意见综合得出的；代表着信息安全工程领域的最佳实践；并且是过程区域（Process Areas，PA ）的强制项。

83. 层次化的文档是信息安全管理体系《Information Security 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》
解释：正确答案为 D。一级文件中一般为安全方针、策略文件；二级文件中一般为管理规范制度；三级文件一般为操作手册和流程；四级文件一般表单和管理记录。

84. 信息安全管理体系（information Security 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（Do），下面给出了一些备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实施风险再评估选的活动，选项（）描述了在此阶段组织应进行的活动。
A.①②③④⑤⑥ B.①②③④⑤⑥⑦ C.①②③④⑤⑥⑦⑧ D.①②③④⑤⑥⑦⑧⑨
解释：管理体系包括 PDCA（Plan-Do-Check-Act）四个阶段，题干中 1-7 的工作都属于管理体系的实施阶段（D-Do），而 8 和 9 属于检查阶段（C-Check）。

85. 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
解释：答案为 C。

86. 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需求和设计阶段增加一定安全措施，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（SDL)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。
解释：答案为 B。A-现代软件工程体系中软件最重要的阶段为设计阶段。C-SDL 最大的特点是增加了安全培训和应急响应。D-第三方测试是必要的软件安全测试类型。

87. 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 WEB 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

解释：答案为 C。

88. 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 SQL 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。
解释：C 有关，ABD 与软件安全开发无关。

89. 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**不在**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
解释：D 属于 ARM 系统，不属于 WEB 安全领域。

90. 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
解释：HTTPS 具有数据加密机制。

91. 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，而不应用定性风险分析
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
解释：实际工作中根据情况选择定量、定性或定量与定性相结合。

92. 小李去参加单位组织的信息安全管理体系（Information Security Management System. ISMS）的理解画了一下一张图(图中包括了规划建立、实施运行、(）、保持和改进)，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
解释：管理体系 PDCA 分别指的阶段是：P-规划建立、D-实施运行、C-监视和评审、A-保持和改进。

93. 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》
解释：答案为 B。

94. 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
解释：指纹识别系统存在安全威胁问题，同时存在着错误拒绝率和错误接受率的问题。

95. 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. 《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》
解释：《国家信息化领导小组关于加强信息安全保障工作的意见》（中办 2003 年 27 号文件）规定了信息安全工作的原则，例如立足国情、以我为主、坚持技管并重等。

96. 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
解释：A 为国标推荐标准；B 为国标强制标准；C 为地方标准；D 为国标指导标准。

97. 微软 SDL 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. 要求阶段 B. 设计阶段 C. 实施阶段 D. 验证阶段
解释：弃用不安全的函数为编码实施阶段。

98. 由于频繁出现计算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
解释：统一采用 Windows8 系统对软件安全无帮助。

99. 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(IATF)，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
解释：A 错误，因为 IATF 不用于代码审核；C 错误，因为人工和攻击相结合；D 错误，安全测试由需求确定。

100. 微软提出了 STRIDE 模型，其中 R 是 Repudiation(抵赖)的缩写，此项错误的是（）
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 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
解释：R-抵赖是无法通过过滤、流控和隐私保护实现的，R-抵赖的实现方式包括数字签名、安全审计、第三方公证。