信息安全专业人员知识测试试题（三）

1. 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
解释：SYSTEM 权限是最大权限，答案为 D。

2. 主机 A 向主机 B 发出的数据采用 AH 或 ESP 的传输模式对经过互联网的数据流量进行保护时，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　　C、192. 168. 0. 0～192. 168. 255. 255
B. 172. 16. 0. 0～172. 31. 255. 255　　D. 不在上述范围内
解释：采用传输模式则没有地址转换，那么 A、B 主机应为公有地址。

3. 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
解释：根据题干是采用 HTTP 的协议导致的，则答案为 A。

4. 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
解释：题干中针对的是传统防火墙，而 SQL 注入防护是 WAF 的主要功能。

5. 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
解释：可信计算平台出现后不会取代传统的安全防护体系和方法。

6. 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. - rwx r-x r-x 3 user admin 1024 Sep 13 11：58 test　　C. - rwx r-x r-x 3 admin user 1024 Sep 13 11：58 test
B. d rwx r-x r-x 3 user admin 1024 Sep 13 11：58 test　　D. d rwx r-x r-x 3 admin user1024 Sep 13 11：58 test
解释：根据题干本题选 A。

7. 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. Inet.conf
解释：根据题干本题选择 A。

8. 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　　C. 不使用管理员权限直接连接数据库系统
B. 对存储的敏感数据进行安全加密　　D. 定期对数据库服务器进行重启以确保数据库运行良好
解释：D 属于运行安全操作，不属于安全防护策略。

9. 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
解释：A 是 SQL 注入；B 是脚本攻击；C 为缓冲区溢出;D 漏洞解释。

10. 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
解释：C 是错误的，应该是最小化端口和服务。

11. 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
解释：C 为正确答案。

12. 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
解释：代码注入文本文件中不能执行。

13. 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
解释：答案为 D。

14. 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
解释：发送大量的 ICMP 回应请求为 ICMP Flood。

15. 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
解释：Teardrop 属于碎片攻击，不属于流量型拒绝服务攻击。

16. 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
解释：D 为正确答案。

17. 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
解释：UDP 协议无流量控制，超时重发等机制。

18. 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
解释：项目管理受项目资源的约束。

19. 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

解释：协调运营商对域名解析服务器进行加固是 DNS 防护的主要手段。

20. 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
解释：D 为源代码审核工作内容描述。

21. 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
解释：持续改进信息安全管理过程属于处置(ACT)阶段。

22. 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
解释：业务特性从机构的业务内容和业务流程获取。

23. 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
解释：“安全产品选择”是为了进行风险处理。

24. 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 C．一个人有且仅有其执行岗位所足够的许可和权限
B．对重要的工作进行分解，分配给不同人员完成 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
解释：C 是“最小特权”的解释；A 描述的是轮岗；B 描述的是权限分离；D 描述的是防止权限蔓延。

25. 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 C．基于模型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 D．基于经验的风险评估与管理工具
解释：D 基于经验的风险评估工具不存在。

26. 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
解释：C 是监理工程师的职责。

27. 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
解释：等级保护三级系统一年测评一次，四级系统每半年测评一次。

28. 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
解释：D 为绝密级。

29. 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 C．创建安全健康的网络环境
B．重点保障基础信息网络和重要信息系统安全 D．提高个人隐私保护意识
解释：提高个人隐私保护意识不属于（2003 年）我国加强信息安全保障工作的总体要求。

30. 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

解释：C 为正确描述。

31. 某单位信息安全岗位员工，利用个人业余时间，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
解释：C 为正确描述。

32. 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
解释：A 的正确描述为立足国情，以我为主，坚持以技术和管理并重。

33. 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
解释：建立国家信息安全研究中心不是我国信息安全保障工作的主要内容。

34. 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。
解释：信息安全管理是人员、技术、操作三者紧密结合的系统工程，是一个动态过程。

35. 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
解释：安全需求来源于内部驱动，D 是外部参考要素，不属于信息安全需求的主要来源。

36. 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
解释：B 是错误的，不是按照领导要求进行了部署和配置。

37. 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
解释：C 属于风险评估阶段的准备阶段，不属于题干中的安全需求阶段。

38. 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
解释：正确的做法为“自评估”和“检查评估”相互结合和互为补充。

39. 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
解释：定性分析不能靠直觉、不能随意。

40. 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
解释：通常情况下信息安全风险评估工具不包括经验工具，环境评估工具。

41. 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
解释：自评估可以委托社会风险评估服务机构来实施。

42. 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，无特殊理由单位均应选择检查评估，以保证安全效果
解释：A 为正确答案。

43. 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(Exposure Factor，EF)是 25%，年度发生率(Annualized Rate of Occurrence，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
解释：计算方法为 200 万*25%*0.1=5 万。

44. 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
解释：《风险评估方案》属于风险评估准备阶段的结果。

45. 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 41 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()
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
解释：风险要素包括资产、威胁、脆弱性、安全措施。

46. 风险要素识别是风险评估实施过程中的一个重要步骤，有关安全要素，请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
解释：风险要素包括资产、威胁、脆弱性、安全措施。

47. 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
解释：《已有安全措施列表》属于风险要素识别识别，风险要素包括资产、威胁、脆弱性、安全措施。

48. 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
解释：信息安全管理体系运行记录需要保护和控制。

49. 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》(GB 50174-2008)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
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
解释：散热为下送风、上回风；侧送风、侧回风。

50. 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
解释：题干描述为符合性检查。

51. 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
解释：系统工程是方法论，不是技术实现。

52. 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。
解释：正确答案为 D。

53. 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
解释：D 为正确的处理方法。

54. 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 C.建立和训练应急响应组织和准备相关的资源
B.编制和管理应急响应计划 D.评估事件的影响范围，增强审计功能、备份完整系统
解释：D 描述的是安全事件发生以后，不是应急响应的准备。

55. 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
解释：通信方使用之前用过的会话秘钥建立会话，会影响通信安全。

56. 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 用同样的方法计算后，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
解释：题干描述的是 C 的解释。

57. 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
解释：SSH 具备数据加密保护的功能。

58. 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
解释：病毒类型不会出现在防火墙的访问控制策略中，病毒类型出现在反病毒网关中。

59. 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
解释：根据题干则答案为 C。

60. 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
解释：设计时提供了用户快捷登录功能，导致大量用户账号被盗用。则答案为 D。

61. 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
解释：题目描述的是软件开发的深度防御思想应用。

62. 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。
解释：威胁就是漏洞是错误的。

63. 为保障系统安全，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
解释：工作中不应该在系统正常业务运行高峰期进行渗透测试。

64. 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”
解释：CMM 的产生是因为过程控制和管理落后引起的。

65. 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()?
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
解释：A 不属于安全配置，而属于部署环境选择。

66. 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
解释：题干描述的是完整性。

67. 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
解释：答案为 C。

68. 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
解释：工业和信息化部牵头成立“国家网络应急中心”。

69. 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）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
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
解释：信息安全需求来自于法律法规标准符合性要求、业务发展要求、风险评估结果。

70. 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
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。

71. 关于我国信息安全保障的基本原则，下列说法中不正确的是：
A. 要与国际接轨，积极吸收国外先进经验并加强合作，遵循国际标准和通行做法，坚持管理与技术并重
B. 信息化发展和信息安全不是矛盾的关系，不能牺牲一方以保证另一方
C. 在信息安全保障建设的各项工作中，既要统筹规划，又要突出重点
D. 在国家信息安全保障工作中，要充分发挥国家、企业和个人的积极性，不能忽视任何一方的作用。
解释：我国信息安全保障首先要遵循国家标准。

72. 2005 年，RFC4301（Request for Comments 4301:Security Architecture for the Internet 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）位流量提供安全业务。请问此类 RFC 系列标准建议是由下面哪个组织发布的（）。
A.国际标准化组织（International Organization for Standardization，ISO）

B.国际电工委员会（International Electrotechnical Commission，IEC）
C.国际电信联盟远程通信标准化组织（ITU Telecommunication Standardization Secctor，ITU-T）
D. Internet 工程任务组（Internet Engineering Task Force，IETF）
解释：D 为正确答案。

73. 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：D 为正确答案。

74. 应急响应是信息安全事件管理的重要内容之一。关于应急响应工作，下面描述错误的是（ ）。
A. 信息安全应急响应，通常是指一个组织为了应对各种安全意外事件的发生所采取的防范措施。即包括预防性措施，也包括事件发生后的应对措施
B. 应急响应工作有其鲜明的特点：具有高技术复杂性与专业性、强突发性、对知识经验的高依赖性，以及需要广泛的协调与合作
C. 应急响应是组织在处置应对突发/重大信息安全事件时的工作，其主要包括两部分工作：安全事件发生时的正确指挥、事件发生后全面总结
D. 应急响应工作的起源和相关机构的成立和 1988 年 11 月发生的莫里斯蠕虫病毒事件有关，基于该事件，人们更加重视安全事件的应急处置和整体协调的重要性
解释：应急响应是安全事件发生前的充分准备和事件发生后的响应处理，准备、检测、遏制、根除、恢复、总结。

75. PDCERF 方法是信息安全应急响应工作中常用的一种方法，它将应急响应分成六个阶段。其中，主要执行如下工作应在哪一个阶段：关闭信息系统、和/或修改防火墙和路由器的过滤规则，拒绝来自发起攻击的嫌疑主机流量、和/或封锁被攻破的登录账号等（）
A. 准备阶段 B. 遏制阶段 C. 根除阶段 D. 检测阶段
解释：拒绝来自发起攻击的嫌疑主机流量等做法属于遏制阶段的工作。

76. 在网络信息系统中对用户进行认证识别时，口令是一种传统但仍然使用广泛的方法，口令认证过程中常常使用静态口令和动态口令。下面找描述中错误的是（ ）
A. 所谓静态口令方案，是指用户登录验证身份的过程中，每次输入的口令都是固定、静止不变的
B. 使用静态口令方案时，即使对口令进行简单加密或哈希后进行传输，攻击者依然可能通过重放攻击来欺骗信息系统的身份认证模块
C.动态口令方案中通常需要使用密码算法产生较长的口令序列，攻击者如果连续地收集到足够多的历史口令，则有可能预测出下次要使用的口令
D. 通常，动态口令实现方式分为口令序列、时间同步以及挑战/应答等几种类型
解释：动态口令方案要求其口令不能被收集和预测。

77. “统一威胁管理”是将防病毒，入侵检测和防火墙等安全需求统一管理，目前市场上已经出现了多种此类安全设备，这里“统一威胁管理”常常被简称为（ ）
A. UTM B. FW C. IDS D. SOC
解释：答案为 A。

78. 某网络安全公司基于网络的实时入侵检测技术，动态监测来自于外部网络和内部网络的所有访问行为。当检测到来自内外网络针对或通过防火墙的攻击行为，会及时响应，并通知防火墙实时阻断攻击源，从而进一步提高了系统的抗攻击能力，更有效地保护了网络资源，提高了防御体系级别。但入侵检测技术不能实现以下哪种功能（ ）。
A. 检测并分析用户和系统的活动
B. 核查系统的配置漏洞，评估系统关键资源和数据文件的完整性
C. 防止 IP 地址欺骗
D. 识别违反安全策略的用户活动
解释：入侵检测技术是发现安全攻击，不能防止 IP 欺骗。

79. Gary McGraw 博士及其合作者提出软件安全 BSI 模型应由三根支柱来支撑，这三个支柱是（ ）。
A. 源代码审核、风险分析和渗透测试
B. 风险管理、安全接触点和安全知识
C. 威胁建模、渗透测试和软件安全接触点
D. 威胁建模、源代码审核和模糊测试
解释：BSI 的模型包括风险管理、安全接触点和安全知识。

80. 以下哪一项不是常见威胁对应的消减措施：
A. 假冒攻击可以采用身份认证机制来防范
B. 为了防止传输的信息被篡改，收发双方可以使用单向 Hash 函数来验证数据的完整性
C. 为了防止发送方否认曾经发送过的消息，收发双方可以使用消息验证码来防止抵赖

D. 为了防止用户提升权限，可以采用访问控制表的方式来管理权限
解释：消息验证码不能防止抵赖，而是提供消息鉴别、完整性校验和抗重放攻击。

81. 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. 通过异常样本重视异常，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 是模糊测试的正确解释。

82. 国务院信息化工作办公室于 2004 年 7 月份下发了《关于做好重要信息系统灾难备份工作的通知》，该文件中指出了我国在灾备工作原则，下面哪项不属于该工作原则（ ）
A. 统筹规划 B. 分组建设 C. 资源共享 D. 平战结合
解释：灾备工作原则包括统筹规划、资源共享、平战结合。

83. 关于信息安全管理体系（Information Security Management Systems,ISMS）,下面描述错误的是（ ）。
A. 信息安全管理体系是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系，包括组织架构、方针、活动、职责及相关实践要素
B. 管理体系（Management Systems）是为达到组织目标的策略、程序、指南和相关资源的框架，信息安全管理体系是管理体系思想和方法在信息安全领域的应用
C. 概念上，信息安全管理体系有广义和狭义之分，狭义的信息安全管理体系是指按照 ISO27001 标准定义的管理体系，它是一个组织整体管理体系的组成部分
D. 同其他管理体系一样，信息安全管理体系也要建立信息安全管理组织机构，健全信息安全管理制度、构建信息安全技术防护体系和加强人员的安全意识等内容
解释：完成安全目标所用各类安全措施的体系。

84. 二十世纪二十年代，德国发明家亚瑟 谢尔比乌斯发明了 Engmia 密码机，按照密码学发展历史阶段划分，这个阶段属于（）
A、古典密码阶段。这一阶段的密码专家常常靠直觉和技术来设计密码，而不是凭借推理和证明，常用的密码运算方法包括替代方法和转换方法（）
B、近代密码发展阶段。这一阶段开始使用机械代替手工计算，形成了机械式密码设备和更进一步的机电密码设备
C、现代密码学的早起发展阶段。这一阶段以香农的论文“保密系统的通信理论”为理论基础，开始对密码学的科学探索
D、现代密码学的近期发展阶段。这一阶段以公钥密码思想为标志，引发了密码学历
解释：根据密码学发展阶段的知识点，Engmia 密码机属于近代密码学发展阶段的产物。

85. 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 400 万元人民币，暴露系数是 25%，年度发生率为 0.2，那么小王计算的年度预期损失应该是（）
A、100 万元人民币 B、400 万元人民币 C、20 万元人民币 D、180 万元人民币
解释：根据 ALE=SLE*ARO=AV*EF*ARO 的公式进行计算。

86. 小牛在对某公司的信息系统进行风险评估后，因考虑到该业务系统中部分涉及金融交易的功能模块风险太高，他建议该公司以放弃这个功能模块的方式来处理风险，请问这种风险处置的方法是（）
A、降低风险 B、规避风险 C、放弃风险 D、转移风险
解释：风险处理方式包括降低、规避、接受和转移四种方式。

87. 关于信息安全事件和应急响应的描述不正确的是（）
A、信息安全事件，是指由于自然或人为以及软、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事件
B、至今已有一种信息安全策略或防护措施，能够对信息及信息系统提供绝对的保护，这就使得信息安全事件的发生是不可能的
C、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
D、应急响应工作与其他信息安全管理工作将比有其鲜明的特点：具有高技术复杂性志专业性、强突发性、对知识经验的高依赖性，以及需要广泛的协调与合作
解释：目前不存在一种信息安全策略或防护措施，能够对信息及信息系统提供绝对的保护。

88. 目前，很多行业用户在进行信息安全产品选项时，均要求产品需通过安全测评，关于信息安全产品测评的意义，下列说法中不正确的是（）
A、有助于建立和实施信息安全产品的市场准入制度
B、对用户采购信息安全产品、设计、建设、使用和管理安全的信息系统提供科学公正的专业指导

C、对信息安全产品的研究、开发、生产以及信息安全服务的组织提供严格的规范引导和质量监督
D、打破市场垄断，为信息安全产品发展创造一个良好的竞争环境
解释：题干中信息安全产品测评的主要目的是安全作用，不是经济作用。

89. 若一个组织声称自己的 ISMS 符合 ISO/TEC27001 或 GB22080 标准要求，其信息安全控制措施通常在以下方面实施常规控制，不包括哪一项（）
A、信息安全方针、信息安全组织、资产管理
B、人力资源安全、物理和环境安全、通信和操作管理
C、访问控制、信息系统获取、开发和维护、符合性
D、规划与建立 ISMS
解释：D 属于 ISMS 的 Plan 工作阶段，不属于措施。

90. 信息安全事件和分类方法有多种，依据 GB/Z 20986-2007《信息安全技术自信安全事件分类分级指南》，信息安全事件分为 7 个基本类别，描述正确的是（）
A、有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件
B、网络贡献事件、拒绝服务攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件
C、网络攻击事件、网络钓鱼事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件
D、网络攻击事件、网络扫描窃听事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件
解释：根据标准知识点，安全事件分为：有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件。

91. 王工是某单位的系统管理员，他在某次参加了单位组织的风险管理工作时，根据任务安排，他使用了 Nessus 工具来扫描和发现数据库服务器的漏洞，根据风险管理的相关理论，他这个是扫描活动属于下面哪一个阶段的工作（）
A、风险分析 B、风险要素识别 C、风险结果判定 D、风险处理
解释：漏洞扫描属于风险要素的脆弱性要素识别，风险要素包括资产、威胁、脆弱性、安全措施。

92. 某集团公司信息安全管理员根据领导安排制定了一下年度的培训工作计划、提出了四大培训任务目标，关于这四个培训任务和目标，作为主管领导，以下选项中最合理（正确）的是（）
A、由于网络安全上升到国家安全的高度，因此网络安全必须得到足够的重视，因此安排了对集团公司下属公司的总经理(一把手)的网络安全法培训
B、对下级单位的网络安全管理人员实施全面安全培训，计划全员通过 CISP 持证培训以确保人员能力得到保障
C、对其他信息化相关人员(网络管理员、软件开发人员)也进行安全基础培训，使相关人员对网络安全有所了解
D、对全体员工安排信息安全意识及基础安全知识培训，安全全员信息安全意识教育
解释：对主管领导来讲，主要是培训网络安全法。

93. 应急响应是信息安全事件管理的重要内容。基于应急响应工作的特点和事件的不规则性，事先创定出事件应急响应方法和过程，有助于一个组织在事件发生时阻止混乱的发生成是在混乱状态中迅速恢复控制，将损失和负面影响降到最低。应急响应方法和过程并不是唯一的。一种被广为接受的应急响应方法是将应急响应管理过程分为 6 个阶段，为准备→检测→遏制-，根除→恢复→跟踪总结。请问下列说法有关于信息安全应急响应管理过程错误的是( ):
A、确定重要资产和风险，实施针对风险的防护措施是信息安全应急响应规划过程中最关键的步骤
B、在检测阶段，首先要进行监测、报告及信息收集
C、遏制措施可能会因为事件的类别和级别不同而完全不同。常见的遏制措施有完全关闭所有系统、拔掉网线等
D、应按照应急响应计划中事先制定的业务恢复优先顺序和恢复步骤，顺次恢复相关的系统
解释：不能完全关闭系统的操作。

94. 某市环卫局网络建设是当地政府投资的重点项目。总体目标就是用于交换式千兆以太网为主干，超五类双绞线作水平布线，由大型交换机和路由器连通几个主要的工作区域，在各区域建立一个闭路电视监控系统，再把信号通过网络传输到各监控中心，其中对交换机和路由器进行配置是网络安全中的一个不可缺少的步骤，下面对于交换机和路由器的安全配置，操作错误的是( )
A、保持当前版本的操作系统，不定期更新交换机操作系统补丁
B、控制交换机的物理访问端口，关闭空闲的物理端口
C、带外管理交换机，如果不能实现的话，可以利用单独的 VLAN 号进行带内管理
D、安全配置必要的网络服务，关闭不必要的网络服务
解释：交换机和路由器的管理包括了版本更新，也包括了补丁管理。

95. 在某信息系统的设计中，用户登陆过程是这样的：（1）用户通过 HTTP 协议访问信息系统；（2）用户在登陆页面输入用户名和口令；（3）信息系统在服务器端检查用户名和密码的正确性，如果正确，则鉴别完成。可以看出，这个鉴别过程属于（）。
A. 单向鉴别 B. 双向鉴别 C. 三向鉴别 D. 第三方鉴别

答案：

96. PKI 的主要理论基础是（）。

A.对称密码算法 B.公钥密码算法 C.量子密码 D.摘要算法

答案：

97. 组织第一次建立业务连续性计划时，最为重要的活动是：

A.制定业务连续性策略 B.进行业务影响分析 C.进行灾难恢复演练 D.构建灾备系统

答案：

98. 防止非法授权访问数据文件的控制措施，哪项是最佳的方式：

A.自动文件条目 B.磁带库管理程序 C.访问控制软件 D.锁定库

答案：

99. 白盒测试的具体优点是：

A.其检查程序是否可与系统的其他部分一起正常运行

B.在不知程序内部结构下确保程序的功能性操作有效

C.其确定程序准确性成某程序的特定逻辑路径的状态

D.其通过严格限制访问主机系统的受控或虚拟环境中执行对程序功能的检查

答案：

100. 为某航空公司的订票系统设计业务连续性计划时，最适用于异地数据转移/备份的方法是：

A.文件映像处理 B.电子链接 C.硬盘镜像 D.热备援中心配置

答案：