信息安全专业人员知识测试试题（五）

1. CC 标准是目前系统安全认证方面最权威的标准，以下哪一项没有体现 CC 标准的先进性：
A. 结构的开放性
B. 表达方式的通用性
C. 独立性
D. 实用性

2. 根据《信息安全等级保护管理办法》、《关于开展信息安全等级保护测评体系建设试点工作的通知》（公信安[2009]812 号），关于推动信息安全等级保护（ ）建设和开展（ ）工作的通知（公信安[2010]303 号）等文件，由公安部（ ）对等级保护测评机构管理，接受测评机构的申请、考核和定期（ ），对不具备能力的测评机构则（ ）
A.等级测评；测评体系；等级保护评估中心；能力验证；取消授权
B.测评体系；等级保护评估中心；等级测评；能力验证；取消授权
C.测评体系；等级测评；等级保护评估中心；能力验证；取消授权
D.测评体系；等级保护评估中心；能力验证；等级测评；取消授权

3. 以下哪个现象较好的印证了信息安全特征中的动态性（ ）
A.经过数十年的发展，互联网上已经接入了数亿台各种电子设备
B 刚刚经过风险评估并针对风险采取处理措施后，仅一周新的系统漏洞使得信息系统面临新的风险
C 某公司的信息系统面临了来自美国的“匿名者”黑客组织的攻击
D.某公司尽管部署了防火墙、防病毒等安全产品，但服务器中数据仍产生了泄露

4. 老王是某政府信息中心主任。以下哪项项目是符合《保守国家秘密法》要求的（ ）
A.老王安排下属小李将损害的涉密计算机某国外品牌硬盘送到该品牌中国区维修中心修理
B.老王要求下属小张把中心所有计算机贴上密级标志
C.老王每天晚上 12 点将涉密计算机连接上互联网更新杀毒软件病毒库
D.老王提出对加密机和红黑电源插座应该与涉密信息系统同步投入使用

5. 关于计算机取取证描述不正确的是（）
A.计算机取证是使用先进的技术和工具，按照标准规程全面的检查计算机系统以提取和保护有关计算机犯罪的相关证据的活动
B.取证的目的包括通过证据，查找肇事者，通过证据推断犯罪过程，通过证据判断受害者损失程度及涉及证据提供法律支持
C.电子证据是计算机系统运行过程中产生的各种信息记录及存储的电子化资料及物品，对于电子证据取证工作主要围绕两方面进行**证据的获取和证据的保护**
D.计算机取证的过程，可以分为准备，保护，提取，分析和提交五个步骤

6. （ ）第 23 条规定存储、处理国家机秘密的计算机信息系统（以下简称涉密信息系统），按照（ ）实行分级保护，（ ）应当按照国家保密标准配备保密设施、设备。（ ）、设备应当与涉密信息系统同步规划、同步建设、同步运行（三同步）。涉密信息系统应当按照规定，经（ ）后方可投入使用。
A.《保密法》；涉密程度；涉密信息系统；保密设施；检查合格
B.《国家保密法》；涉密程度；涉密系统；保密设施；检查合格
C.《网络保密法》；涉密程度；涉密系统；保密设施；检查合格
D.《安全保密法》；涉密程度，涉密信息系统；保密设施；检查合格

7. Linux 系统的安全设置主要从磁盘分区、账户安全设置、禁用危险服务、远程登录安全、用户鉴别安全、审计策略、保护 root 账户、使用网络防火墙和文件权限操作共 10 个方面来完成。小张在学习了 Linux 系统安全的相关知识后，尝试为自己计算机上的 Linux 系统进行安全配置。下列选项是他的部分操作，其中不合理的是（ ）。
A. 编辑文件/etc/passwd，检查文件中用户 ID，禁用所有 ID=0 的用户

B. 编辑文件/etc/ssh/sshd _config，将 Permit RootLogin 设置为 no
C. 编辑文件/etc/pam.d/system~auth，设置 auth required pam tally. so onerr=fail deny=6 unlock_time-300
编辑文件/etc/profile，设置 TMOUT=600

8. PDCA 循环又叫戴明环，是管理学常用的一种模型。关于 PDCA 四个字母，下面理解错误的是（ ）
A.P 是 Plan，指分析问题、发现问题、确定方针、目标和活动计划
B.D 是 Do，指实施、具体运作，实现计划中的内容
C.C 是 Check，指检查、总结执行计划的结果，明确效果，找出问题
D.A 是 Aim，指瞄准问题，抓住安全事件的核心，确定责任

9. 在国家标准 GB/T 20274. 1-2006《信息安全技术信息系统安全保障评估框架第一部分：简介和一般模型》中，信息系统安全保障模型包含哪几个方面？（ ）
A.保障要素、生命周期和运行维护
B.保障要素、生命周期和安全特征
C.规划组织、生命周期和安全特征
D.规划组织、生命周期和运行维护

10. 目前，信息系统面临外部攻击者的恶意攻击威胁，从成胁能力和掌握资源分，这些威胁可以按照个人或胁、组织威胁和国家威胁三个层面划分，则下面选项中属于组织威胁的是（ ）
A. 喜欢恶作剧、实现自我挑战的娱乐型黑客
B. 实施犯罪、获取非法经济利益网络犯罪团伙
C. 搜集政治、军事、经济等情报信息的情报机构
D. 巩固战略优势，执行军事任务、进行目标破坏的信息作战部队

11. 若一个组织声称自己的 ISMS 符合 ISO/IEC 27001 或 GB/T22080 标准要求，其信息安全控制措施通常需要在资产管理方面安施常规控制，资产管理包含对资产负责和信息分类两个控制目标。信息分类控制的目标是为了确保信息受到适当级别的保护，通常采取以下哪项控制措施（ ）
A. 资产清单
B. 资产责任人
C. 资产的可接受使用
D. 分类指南，信息的标记和处理

12. 有关质量管理，错误的理解是（ ）。
A.质量管理是与指挥和控制组织质量相关的一系列相互协调的活动，是为了实现质量目标，而进行的所有管理性质的活动
B.规范质量管理体系相关活动的标准是 ISO 9000 系列标准
C 质量管理体系将资源与结果结合，以结果管理方法进行系统的管理
D 质量管理体系从机构，程序、过程和总结四个方面进行规范来提升质量

13. 在某信息系统的设计中，用户登录过程是这样的： (1)用户通过 HTTP 协议访问信息系统； (2)用户在登录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

14. 随机进程名称是恶意代码迷惑管琊员和系统安全检查人员的技术手段之一，以下对于随机进程名技术。描述正确的是（ ）。
A. 随机进程名技术虽然每次进程名都是随机的，但是只要找到了进程名称，就找到了恶意代码程序本身
B. 恶意代码生成随机进程名称的目的是使过程名称不固定，因为杀毒软件是按照进程名称进行病毒进程查杀
C. 恶意代码使用随机进程名是通过生成特定格式的进程名称，使进程管理器中看不到恶意代码的进程
D. 随机进程名技术每次启动时随机生成恶意代码进程名称，通过不固定的进程名称使自己不容易被发现真实的恶意代码程序名称

15. 随着即时通讯软件的普及使用，即时通讯软件也被恶意代码利用进行传播，以下哪项功能不是恶意代码利用即时通讯进行传播的方式

A. 利用即时通讯软件的文件传送功能发送带恶意代码的可执行文件 1

B. 利用即时通讯软件发送指向恶意网页的 URL 2

C. 利用即时通讯软件发送指向恶意地址的二维码 3

D. 利用即时通讯发送携带恶意代码的 JPG 图片 1

16. GB/T 22080-2008 《信息技术 安全技术 信息安全管理体系要求》指出，建立信息安全管理体系应参照 PDCA 模型进行，即信息安全管理体系应包括建立 ISMS、 实施和运行 ISMS、监视和评审 ISMS、 保持和改进 ISMS 等过程，并在这些过程中应实施若干活动。请选出以下描述错误的选项（ ）。

A.“制定 ISMS 方针”是建立 ISMS 阶段工作内容

B.“安施培训和意识教育计划”是实施和运行 ISMS 阶段工作内容

C.“进行有效性测量”是监视和评审 ISMS 阶段工作内容

D.“实施内部审核”是保持和改进 ISMS 阶段工作内容

17. 某单位需要开发一个网站，为了确保开发出安全的软件。软件开发商进行了 OA 系统的威胁建模，根据威胁建模，SQL 注入是网站系统面临的攻击威胁之一， 根据威胁建模的消减威胁的做法。以下哪个属于修改设计消除威胁的做法（ ）

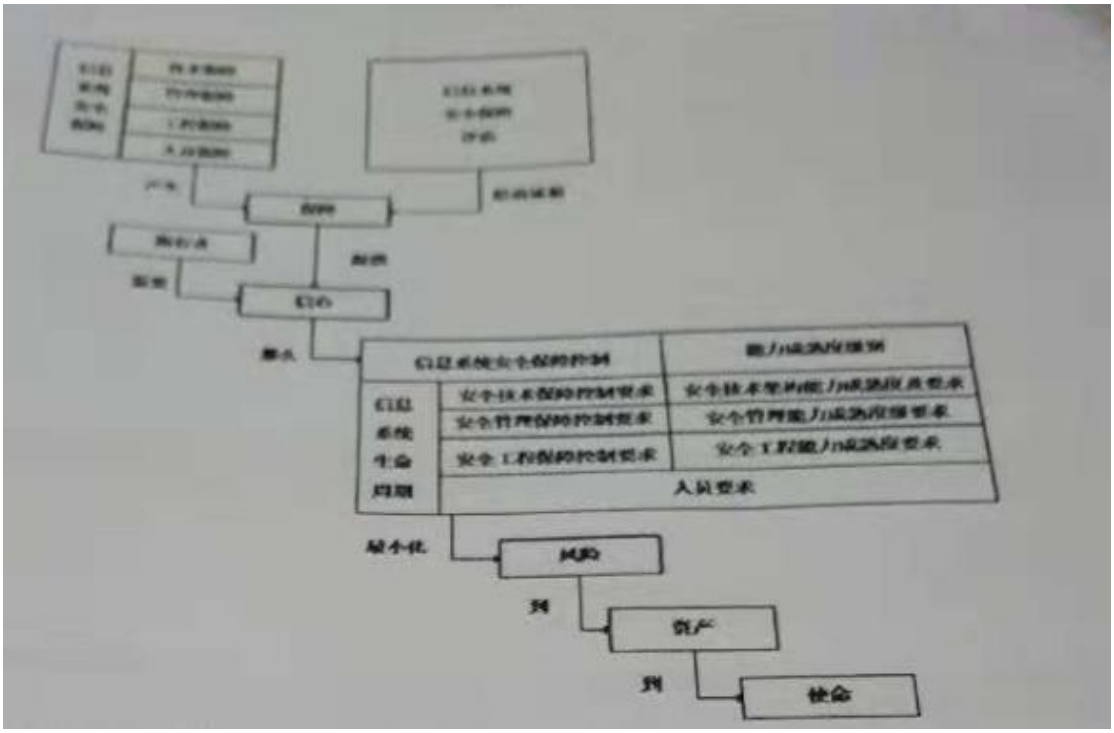
A. 在编码阶段程序员进行培训，避免程序员写出存在漏洞的代码

B. 对代码进行严格检查，避免存在 SQL 注入漏洞的脚本被发布

C. 使用静态发布，所有面向用户发布的数据都使用静态页面

D. 在网站中部署防 SQL 注入脚本，对所有用户提交数据进行过滤

18. 信息系统安全保障评估概念和关系如图所示。信息系统安全保障评估，就是在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估。通过信息系统安全保障评估所搜集的（ ），向信息系统的所有相关方提供信息系统的（ ）能够实现其安全保障策略，能够将其所面临的风险降低到其可接受的程度的主观信心。信息系统安全保障评估的评估对象是（ ），信息系统不仅包含了仅讨论技术的信息技术系统，还包括同信息系统所处的运行环境相关的人和管理等领域。信息系统安全保障是一个动态持续的过程，涉及信息系统整个（ ），因此信息系统安全保障的评估也应该提供一种（ ）的信心。



A. 安全保障工作；客观证据；信息系统；生命周期；动态持续

B. 客观证据；安全保障工作；信息系统；生命周期；动态持续

C. 客观证据；安全保障工作；生命周期；信息系统；动态持续
D. 客观证据；安全保障工作；动态持续；信息系统；生命周期

19. 某企业内网中感染了一种依靠移动存储进行传播的特洛伊木马病毒，由于企业部署的杀毒软件，为了解决该病毒在企业内部传播，作为信息化负责人，你应采取以下哪项策略()
A.更换企业内部杀毒软件，选择一个可以查杀到该病毒的软件进行重新部署
B.向企业内部的计算机下发策略，关闭系统默认开启的自动播放功能
C.禁止在企业内部使用如 U 盘、移动硬盘这类的移动存储介质
D.在互联网出口部署防病毒网关，防止来自互联网的病毒进入企业内部

20. 分布式拒绝服务（Distributed Denial of Service, DDos）攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台。对一个或多个目标发动 DDoS 攻击，从而成倍地提高拒绝服务攻击的威力。一般来说，DDoS 攻击的主要目的是破坏目标系统的（）
A. 保密性
B. 完整性
C. 可用性
D. 真实性

21. 作为信息安全从业人员，以下哪种行为违反了 CISP 职业道德准侧（）
A. 抵制通过网络系统侵犯公众合法权益
B. 通过公众网络传播非法软件
C. 不在计算机网络系统中进行造谣、欺诈、诽谤等活动
D. 帮助和指导信息安全同行提升信息安全保障知识和能力。

22. Apache HTTP Server（简称 Apache）是个开放源码的 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，应当采取以下哪种措施()
A .不选择Windons平台，应选择在Linux平台下安装使用
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

23. 安全漏洞产生的原因不包括以下哪一点()
A. 软件系统代码的复杂性
B. 软件系统市场出现信息不对称现象
C. 复杂异构的网络环境
D. 攻击者的恶意利用

24. 某 IT 公司针对信息安全事件已经建立了完善的预案，在年度企业信息安全总结会上，信息安全管理员对今年应急预案工作做出了四个总结，其中有一项总结工作是错误，作为企业的 CSO，请你指出存在问题的是哪个总结？（）
A. 公司自身拥有优秀的技术人员，系统也是自己开发的，无需进行应急演练工作，因此今年的仅制定了应急演练相关流程及文档，为了不影响业务，应急演练工作不举行
B. 公司制定的应急演练流程包括应急事件通报、确定应急事件优先级应急响应启动实施、应急响应时间后期运维、更新现在应急预案五个阶段，流程完善可用
C. 公司应急预案包括了基本环境类、业务系统、安全事件类、安全事件类和其他类，基本覆盖了各类应急事件类型
D. 公司应急预案对事件分类依据GB/Z 20986 - 2007《信息安全技术信息安全事件分类分级指南》，分为7 个基本类别，预案符合国家相关标准

25. 某软件在设计时，有三种用户访问模式，分别是仅管理员可访问、所有合法用户可访问和允许匿名访问，采用这三种访问模式时，攻击面最高的是()。
A. 仅管理员可访问

B. 所有合法用户可访问
C. 允许匿名
D. 三种方式一样

26. 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，发现当前案例中共有两个重要资产：资产 A1 和资产 A2，其中资产 A1 面临两个主要威胁：威胁 T1 和威胁 T2；而资产 A2 面临一个主要威胁：威胁 T3；威胁 T1 可以利用的资产 A1 存在的两个脆性：脆弱性 V1 和脆弱性 V2； 威胁 T2 可以利用的资产 A1 存在的三个脆弱性：脆弱性 V3、脆弱性 V4 和脆弱性 V5；威胁 T3 可以利用的资产 A2 存在的两个脆弱性：脆弱性 V6 和脆弱性 V7；根据上述条件，请问:使用***相乘法***时，应该为资产 A1 计算几个风险值( )
A. 2
B. 3
C. 5
D. 6
解释：A1面临威胁T1和威胁T2；T1利用V1和V2；T2利用V3,V4和V5。A2面临威胁T3；T3利用V6和V7。
{A1,T1,V1},{A1,T1,V2},{A1,T2,V3},{A1,T2,V4},{A1,T2,V5}

27. 某政府机构委托开发商开发了一个 OA系统。其中公交分发功能使用了FTP协议，该系统运行过程中被攻击者通过FTP对OA系统中的脚本文件进行了篡改，安全专家提出使用Http下载代替FTP功能以解决以上问题，该安全问题的产生主要是在哪个阶段产生的()
A程序员在进行安全需求分析时，没有分析出OA系统开发的安全需求
B. 程序员在软件设计时，没遵循降低攻击面的原则，设计了不安全的功能
C. 程序员在软件编码时，缺乏足够的经验，编写了不安全的代码
D. 程序员在进行软件测试时，没有针对软件安全需求进行安全测试

28. 从SABSA的发展过程，可以看出整个SABSA在安全架构中的生命周期（如下图所示），在此SABSA生命周期中，前两个阶段的过程被归类为所谓的（ ），其次是（ ），它包含了建筑设计中的（ ）、物理设计、组件设计和服务管理设计，再者就是（ ），紧随其后的则是（ ）
A. 设计；战略与规划；逻辑设计；实施；管理与衡量
B. 战略与规划；逻辑设计；设计；实施；管理与衡量
C. 战略与规划；实施；设计；逻辑设计；管理与衡量
D. 战略与规划；设计；逻辑设计；实施；管理与衡量

29. 随着信息安全涉及的范围越来越广，各个组织对信息安全管理的需求越来越迫切。越来越多的组织开始尝试使用参考ISO27001介绍的ISMS来实施信息安全管理体系，提高组织的信息安全管理能力。关于ISMS。下面描述错误的是（ ）。
A. 在组织中，应由*信息技术责任部门(如信息中心)*制定并颁布信息安全方针，为组织的ISMS建设指明方向并提供总体纲领，明确总体要求
B. 组织的管理层应确保ISMS目标和相应的计划得以制定，信息安全管理目标应明确、可度量，风险管理计划应具体，具备可行性
C. 组织的信息安全目标、信息安全方针和要求应传达到全组织范围内。应包括全体员工，同时，也应传达到客户、合作伙伴和供应商等外部各方
D. 组织的管理层应全面了解组织所面临的信息安全风险，决定风险可接受级别和风险可接受准则，并确认接受相关残余风险

30. 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(Exposure Factor,EF)是25%，年度发生率(Annualized Rate of Occurrence, ARO)是0.2,那么小王计算的年度预期损失（Annualized Loss Expectancy, ALE）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

31. 随着信息技术的不断发展，信息系统的重要性也越来越突出，而与此同时，发生的信息安全事件也越来 ，综合分析信息安全问题产生的根源，下面描述正确的是（ ）
A. 信息系统自身存在脆弱性是根本原因。信息系统越来越重要，同时自身在开发、部署和使用过程中存 性，

导致了诸多的信息安全事件发生。因此，杜绝脆弱性的存在是解决信息安全问题的根本所在
B.信息系统面临诸多黑客的威胁，包括恶意攻击者和恶作剧攻击者。信息系统应用越来越广泛，接触 越多，信息系统越可能遭受攻击，因此避免有恶意攻击可能的人接触信息系统就可以解决信息安全问题
C.信息安全问题，产生的根源要从内因和外因两个方面分析，因为信息系统自身存在脆弱性同时外部又有威胁源，从而导致信息系统可能发生安全事件，因此要防范安全风险，需从内外因同时着手
D.信息安全问题的根本原因是内因、外因和人三个因素的综合作用，内因和外因都可能导致安全事件的发生，但最重要的还是人的因素，外部攻击者和内部工作人员通过远程攻击，本地破坏和内外勾结等手段导致安全事件发生，因此对人这个因素的防范应是安全工作重点

32. 在Linux系统中，下列哪项内容不包含在/etc/passwd文件中（）
A. 用户名
B. 用户口令明文
C. 用户主目录
D. 用户登录后使用的 SHELL

33. 即使最好用的安全产品也存在（）。结果，在任何的系统中敌手最终都能够找出一个被开发出的漏洞。一种有效的对策时在敌手和它的目标之间配备多种（）。每一种机制都应包括（）两种手段。
A. 安全机制；安全缺陷；保护和检测
B. 安全缺陷；安全机制；保护和检测
C. 安全缺陷；保护和检测；安全机制；
D. 安全缺陷；安全机制；保护和监测

34. 某攻击者想通过远程控制软件潜伏在某监控方的UNIX系统的计算机中，如果攻击者打算长时间地远程监控某服务器上的存储的敏感数据，必须要能够清除在监控方计算机中存在的系统日志。否则当监控方查看自己的系统日志的时候，就会发现被监控以及访向的痕迹。不属于清除痕迹的方法是()。
A.窃取 root 权限修改 wtmp/wtmpx、utmp/utmpx 和 lastlog 三个主要日志文件
B.采用干扰手段影响系统防火墙的审计功能
C. 保留攻击时产生的临时文件
D. 修改登录日志，伪造成功的登录日志，增加审计难度

35. 信息安全组织的管理涉及内部组织和外部各方两个控制目标。为了实现对组织内部信息安全的有效管理，实施常规的控制措施，不包括哪些选项()
A.信息安全的管理承诺、信息安全协调、信息安全职责的分配
B.信息处理设施的授权过程、保密性协议、与政府部门的联系.
C 与特定利益集团的联系，信息安全的独立评审
D.与外部各方相关风险的识别、处理外部各方协议中的安全问题

36. 按照我国信息安全等级保护的有关政策和标准，有些信息系统只需要自主定级、自主保护，***按照要求向公安机关备案即可，可以不需要上级或主管都门来测评和检查***。此类信息系统应属于：
A.零级系统 B 一级系统 C 二级系统 D.三级系统

37. 小李在检查公司对外服务网站的源代码时，发现程序在发生诸如没有找到资源、数据库连接错误、写临时文件错误等问题时，会将详细的错误原因在结果页面上显示出来。从安全角度考虑，小李决定修改代码。将详细的错误原因都隐藏起来，在页面上仅仅告知用户“抱歉。发生内部错误!”.请问，这种处理方法的主要目的是()。
A 避免缓冲区溢出 B.安全处理系统异常
C 安全使用临时文件 D.最小化反馈信息

38. 关于 ARP 欺骗原理和防范措施，下面理解错误的是( )
A. ARP 欺骗是指攻击者直接向受害者主机发送错误的 ARP 应答报文。使得受害者主机将错误的硬件地址映射关系存到 ARP 缓存中，从而起到冒充主机的目的
B. 单纯利用 ARP 欺骗攻击时，ARP 欺骗通常影响的是内部子网，不能跨越路由实施攻击

C. 解决 ARP 欺骗的一个有效方法是采用“静态”的 APP 缓存，如果发生硬件地址的更改，则需要人工更新缓存
D. 彻底解决 ARP 欺骗的方法是避免使用 ARP 协议和 ARP 缓存。直接采用 IP 地址和其地主机进行连接

39. 组织内人力资源部门开发了一套系统，用于管理所有员工的各种工资、绩效、考核、奖励等事宜。所有员工都可以登录系统完成相关需要员工配合的工作，以下哪项技术可以保证数据的保密性：
A. SSL 加密
B. 双因子认证
C. 加密会话 cookie
D. IP 地址校验

40. 强制访问控制是指主体和客体都有一个固定的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体，具有较高的安全性，适用于专用或对安全性较高的系统。强制访问控制模型有多种类型，如 BLP、Biba、Clark-Willson 和 ChineseWall 等。小李自学了 BLP 模型，并对该模型的特点进行了总结。以下 4 钟对 BLP 模型的描述中，正确的是（ ）：
A. BLP 模型用于保证系统信息的机密性，规则是“向上读，向下写”
B. BLP 模型用于保证系统信息的机密性，规则是“向下读，向上写”
C. BLP 模型用于保证系统信息的完整性，规则是“向上读，向下写”
D. BLP 模型用于保证系统信息的完整性，规则是“向下读，向上写”

41. 一个信息管理系统通常会对用户进行分组并实施访问控制。例如，在一个学校的教务系统中，教师能够录入学生的考试成绩，学生只能查看自己的分数，而学校教务部门的管理人员能够对课程信息、学生的选课信息等内容进行修改。下列选项中，对访问控制的作用的理解错误的是：
A. 对经过身份鉴别后的合法用户提供所有服务
B. 拒绝非法用户的非授权访问请求
C. 在用户对系统资源提供最大限度共享的基础上，对用户的访问权进行管理
D. 防止对信息的非授权篡改和滥用

42. 信息安全风险等级的最终因素是：
A. 威胁和脆弱性
B. 影响和可能性
C. 资产重要性
D. 以上都不对
解释：影响指的就是安全事件的损失，可能性指的是安全事件的可能性。

43. 实施灾难恢复计划之后，组织的灾难前和灾难后运营成本将：
A. 降低
B. 不变（保持相同）
C. 提高
D. 提高或降低（取决于业务的性质）

44. 自主访问控制模型（DAC）的访问控制关系可以用访问控制表（ACL）来表示，该 ACL 利用在客体上附加一个主体明细表的方法来表示访问控制矩阵，通常使用由客体指向的链表来存储相关数据。下面选项中说法正确的是（ ）。
A. ACL 是 Bell-LaPadula 模型的一种具体实现
B. ACL 在删除用户时，去除该用户所有的访问权限比较方便
C. ACL 对于统计某个主体能访问哪些客体比较方便
D. ACL 在增加和修改哪些客体被主体访问比较方便

45. 二十世纪二十年代，德国发明家亚瑟.谢尔比乌斯（Arthur Scherbius）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巧来设计密码，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置换方法
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.现代密码学的早期发展阶段。这一阶段以香农的论文“保密系统的通信理论”（“The Communication Theory of Secret Systems”）为理论基础，开始了对密码学的科学探索。
D.现代密码学的近代发展阶段。这一阶段以公钥密码思想为标准，引发了密码学历史上的革命性的变革，同时，众多的密码算法开始应用于非机密单位和商业场合。

46. 主体和客体是访问控制模型中常用的概念。下面描述中错误的是（ ）
A.主体是访问的发起者，是一个主动的实体，可以操作被动实体的相关信息或数据
B.客体也是一个实体，是操作的对象，是被规定需要保护的资源
C.主体是动作的实施者，比如人、进程或设备等均是主体，这些对象不能被当作客体使用
D.一个主体为了完成任务，可以创建另外的主体，这些主体可以独立运行

47. 数字签名不能实现的安全特性为（ ）
A.防抵赖
B.防伪造
C.防冒充
D.保密通信

48. 在入侵检测（IDS）的运行中，最常见的问题是：（）
A.误报检测
B.接收陷阱消息
C.误拒绝率
D.拒绝服务攻击

49. 什么是系统变更控制中最重要的内容?
A.所有的变更都必须文字化，并被批准
B.变更应通过自动化工具来实施
C.应维护系统的备份
D.通过测试和批准来确保质量

50. IPv4 协议在设计之初并没有过多地考虑安全问题，为了能够使网络方便地进行互联、互通，仅仅依靠 IP 头部的校验和字段来保证 IP 包的安全，因此 IP 包很容易被篡改，并重新计算校验和。IETF 于 1994 年开始制定 IPSec 协议标准，其设计目标是在 IPv4 和 IPv6 环境中为网络层流量提供灵活、透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，保证数据的完整性和机密性，有效抵御网络攻击，同时保持易用性。下列选项中说法错误的是（ ）
A.对于 IPv4, IPSec 是可选的，对于 IPv6，IPSec 是强制实施的。
B. IPSec 协议提供对 IP 及其上层协议的保护。
C. IPSec 是一个单独的协议
D. IPSec 安全协议给出了封装安全载荷和鉴别头两种通信保护机制。

51. 小赵是某大学计算机科学与技术专业的毕业生，在前往一家大型企业应聘时，面试经理要求他给出该企业信息系统访问控制模型的设计思路。如果想要为一个存在大量用户的信息系统实现自主访问控制功能，在以下选项中，从时间和资源消耗的角度，下列选项中他应该采取的最合适的模型或方法是（ ）。
A.访问控制列表（ACL）
B.能力表（CL）
C.BLP 模型
D.Biba 模型

52. 在软件开发过程中，常用图作为描述攻击，如 DFD 就是面向（）分析方法的描述工具，在一套分层 DFD 中，如果某一张图中有 N 个加工（Process）则这张图允许有（）张子图，在一张 DFD 中任意两个加工之间（）。

在画分层 DFD 时，应注意保持（）之间的平衡。DFD 中从系统的输入流到系统的输出流的一连串交换形式一种信息流，这种信息流可分为交换流和事物流两类。
A. 数据流；0^N；有 0 条或多条名字互不相同的数据流；父图与其子图
B. 数据流；I^N；有 0 条或多条名字互不相同的数据流；父图与其子图
C. 字节流；0^N；有 0 条或多条名字互不相同的数据流；父图与其子图
D. 数据流；0^N；有 0 条或多条名字互不相同的数据流；子图之间

53. 社会工程学本质上是一种（），（）通过种种方式来引导受攻击者的（）向攻击者期望的方向发展。罗伯特·B·西奥迪尼（Robert B Cialdini）在科学美国人（2001 年 2 月）杂志中总结对（）的研究，介绍了 6 种“人类天性基本倾向”，这些基本倾向都是（）工程师在攻击中所依赖的（有意思或者无意识的）。
A. 攻击者；心理操纵；思维；心理操纵；社会工程学
B. 攻击者；心理操纵；心理操纵；社会工程学
C. 心理操纵；攻击者；思维；心理操纵；社会工程学
D. 心理操纵；思维；心理操纵；攻击者；社会工程学

54. ITIL 它包含 5 个生命周期，分别是（）、（）、（）、（）、（）.
A. 战略阶段；设计阶段；转换阶段；运营阶段；改进阶段
B. 设计阶段；战略阶段；转换阶段；运营阶段；改进阶段
C. 战略阶段；设计阶段；运营阶段；转换阶段；改进阶段
D. 转换阶段；战略阶段；设计阶段；运营阶段；改进阶段

55. 某公司正在进行 IT 系统灾难恢复测试，下列问题中哪个最应该引起关注()
A. 由于有限的测试时间窗，仅仅测试了最必须的系统，其他系统在今年的剩余时间里陆续单独测试
B. 在测试的过程中，有些备份系统有缺陷或者不能正常工作，从而导致这些系统的测试失败
C. 在开启备份站点之前关闭和保护原生产站点的过程比计划需要多得多的时间
D. 每年都是由相同的员工执行此测试，由于所有的参与者都很熟悉每一个恢复步骤，因而没有使用灾难恢复计划（DRP）文档

56. COBIT（信息和相关技术的控制目标）是国际专业协会 ISACA 为信息技术（IT）管理和 IT 治理创建的良好实践框架。COBIT 提供了一套可实施的“信息技术控制”并围绕 IT 相关流程和推动因素的逻辑框架进行组织。COBIT 模型按照流程，请问，COBIT 组件包括（）、()、（）、（）、（）等部分。
A. 流程描述、框架、控制目标、管理指南、成熟度模型
B. 框架、流程描述、管理目标、控制目标、成熟度模型
C. 框架、流程描述、控制目标、管理指南、成熟度模型
D. 框架、管理指南、流程描述、控制目标、成熟度模型

57. 关于软件安全问题，下面描述错误的是（）
A.软件的安全问题可以造成软件运行不稳定，得不到正确结果甚至崩溃
B.软件的安全问题应该依赖于软件开发的设计、编程、测试以及部署等各个阶段措施解决
C.软件的安全问题可能被攻击者利用后影响人身健康安全
D.软件的安全问题是由程序开发者遗留的，和软件部署运行环境无关

58. 以下哪项是《国家信息化领导小组关于加强信息安全保障工作的意见》的总体方针和要求？
A. 坚持积极攻击、综合防范的方针
B. 全面提高信息安全防护能力
C. 重点保障电信基础信息网络和重要信息系统安全
D. 创建安全健康的网络环境，保障和促进工业化发展，保护公众利益，维护国家安全

59. 随着计算机和网络技术的迅速发展，人们对网络的依赖性达到了前所未有的程度，网络安全也面临着越来越严峻的考验。如何保障网络安全就显得非常重要，而网络安全评估是保证网络安全的重要环节。以下不属于网络安全评估内容的是（）
A.数据加密 B.漏洞检测 C.风险评估 D.安全审计

60. 2006 年 5 月 8 日电，中共中央办公厅、国务院办公厅印发了《2006-2020 年国家信息化发展战略》。全文分（）部分共计约 15000 余字。对国内外的信息化发展做了宏观分析，对我国信息化发展指导思想和战略目标标准要阐述，对我国（）发展的重点、行动计划和保障措施做了详尽描述。该战略指出了我国信息化发展的（），当前我国信息安全保障工作逐步加强。制定并实施了（）,初步建立了信息安全管理体制和（）。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

A. 5 个；信息化；基本形势；国家安全战略；工作机制

B. 6 个；信息化；基本形势；国家信息安全战略；工作机制

C. 7 个；信息化；基本形势；国家安全战略；工作机制

D. 8 个；信息化；基本形势；国家信息安全战略；工作机制

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

A. 任何一个新建用户都需要经过授权才能访问系统中的文件

B. windows 不认为新建立用户 zhang 与原来的用户 zhang 同一个用户，因此无权访问

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

D. 新建的用户 zhang 会继承原来用户的权限，之所以无权访问时因为文件夹经过了加密

62. ISO2007：2013《信息技术-安全技术-信息安全管理体系-要求》为在组织内为建立、实施、保持和不断改进（）制定了要求。ISO27001 标准的前身为（）的 BS7799 标准，该标准于 1993 年由（）立项，于 1995 年英国首次出版 BS7799-1：1995《信息安全管理实施细则》，它提供了一套综合的、由信息安全最佳惯例组成的（），其目的是作为确定工商业信息系统在大多数情况所需控制范围的唯一（），并且适用大、中、小组织。

A. ISMS；德国；德国贸易工业部；实施规则；参考基准

B. ISMS；法国；法国贸易工业部；实施规则；参考基准

C. ISMS；英国；英国贸易工业部；实施规则；参考基准

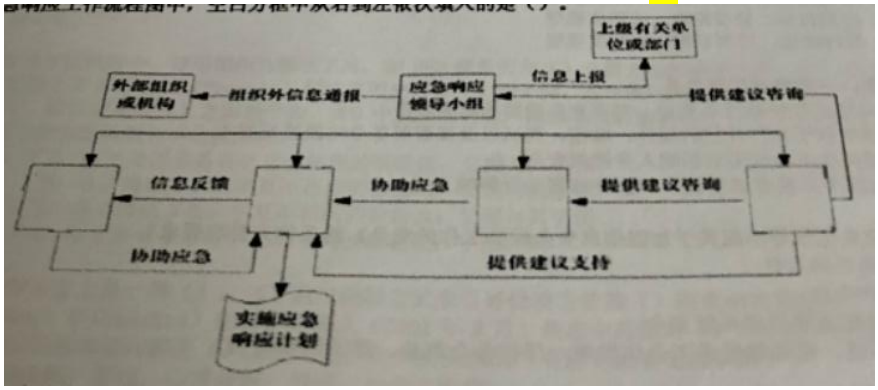
D. ISMS；德国；德国贸易工业部；参考基准；实施规则

63. 终端访问控制器访问控制系统（Terminal Access Controller Access-Control System,TACACS）由 RFC1492 定义，标准的 TACACS 协议只认证用户是否可以登录系统，目前已经很少使用，TACACS+协议由 Cisco 公司提出，主要应用于 Ciso 公司的产品中，运行与 TCP 协议之上。TACACS+协议分为（）两个不同的过程

A. 认证和授权　　B. 加密和认证

C. 数字签名和认证　　D. 访问控制和加密

64. 网络与信息安全应急预案是在分析网络与信息系统突发事件后果和应急能力的基础上，针对可能发生的重大网络与信息系统突发事件，预先制定的行动计划或应急对策。应急预案的实施需要各子系统的相互配合与协调，下面应急响应工作流程图中，空白方框中从右到左依次填入的是（）。



A. 应急响应专家小组、应急响应技术保障小组、应急响应实施小组、应急响应日常运行小组

B. 应急响应专家小组、应急响应实施小组、应急响应技术保障小组、应急响应日常运行小组

C. 应急响应技术保障小组、应急响应专家小组、应急响应实施小组、应急响应日常运行小组
D. 应急响应技术保障小组、应急响应专家小组、应急响应日常运行小组、应急响应实施小组

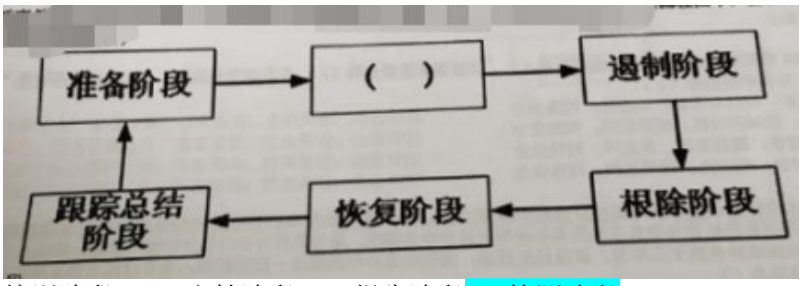
65. 随着计算机在商业和民用领域的应用，安全需求变得越来越多样化，自主访问控制和强制访问控制难以适应需求，基于角色的访问控制(RBAC)逐渐成为安全领域的一个研究热点。RBAC 模型可以分为 RBAC0、RBAC1、RBAC2 和 RBAC3 四种类型，它们之间存在相互包含关系。下列选项中，对它们关系描述错误的是（）。
A. RBAC0 是基于模型，RBAC1、RBAC2 和 RBAC3 都包含 RBAC0
B. RBAC1 在 RBAC0 的基础上，加入了角色等级的概念
C. RBAC2 在 RBAC1 的基础上，加入了约束的概念
D. RBAC3 结合 RBAC1 和 RBAC2，同时具备角色等级和约束

66. 安全漏洞扫描技术是一类重要的网络安全技术。当前，网络安全漏洞扫描技术的两大核心技术是（）。
A. PING 扫描技术和端口扫描技术
B. 端口扫描技术和漏洞扫描技术
C. 操作系统探测和漏洞扫描技术
D. PING 扫描技术和操作系统探测

67. 下列选项中对信息系统审计概念的描述中不正确的是（）
A. 信息系统审计，也可称作 IT 审计或信息系统控制审计
B. 信息系统审计是一个获取并评价证据的过程，审计对象是信息系统相关控制，审计目标则是判断信息系统是否能够保证其安全性、可靠性、经济性以及数据的真实性、完整性等相关属性
C. 信息系统审计师单一的概念，是对会计信息系统的安全性、有效性进行检查
D. 从信息系统审计内容上看，可以将信息系统审计分为不同专项审计，例如安全审计、项目合规审计、绩效审计等

68. 甲公司打算制作网络连续时所需要的插件的规格尺寸、引脚数量和线序情况，甲公司将这个任务委托了乙公司，那么乙公司的设计员应该了解 OSI 参考模型中的哪一层（）
A. 数据链路层 B. 会话层 C. 物理层 D. 传输层

69. 信息安全应急响应，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，既包括预防性措施，也包括事件发生后的应对措施。应急响应方法和过程并不偶是唯一的，在下面的应急响应管理流程中，空白方框处填写正确的是选项是（）



培训阶段 B. 文档阶段 C. 报告阶段 D. 检测阶段

70. 下面哪一项情景属于身份鉴别（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 文档进行加密，以阻止其他人得到这份拷贝后到文档中的内容
C. 用户使用加密软件对自己家编写的 Office 文档进行加密，以阻止其他人得到这份拷贝后到文档中的内容
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记录在系统日志中

71. 终端访问控制器访问控制系统（TERMINAL Access Controller Access-Control System,TACACS），在认证过程中，客户机发送一个 START 包给服务器，包的内容包括执行的认证类型、用户名等信息。START 包只在一个认证会话开始时使用一个，序列号永远为（）.服务器收到 START 包以后，回送一个 REPLY 包，表示认

证继续还是结束。
A．0 B.1 C.2 D.4

72. 为了开发高质量的软件，软件效率成为最受关注的话题。那么开发效率主要取决于以下两点：开发新功能是否迅速以及修复缺陷是否及时。为了提高软件测试的效率，应（）。
A．随机地选取测试数据
B．取一切可能的输入数据为测试数据
C．在完成编码以后制定软件的测试计划
D．选择发现错误可能性最大的数据作为测试用例

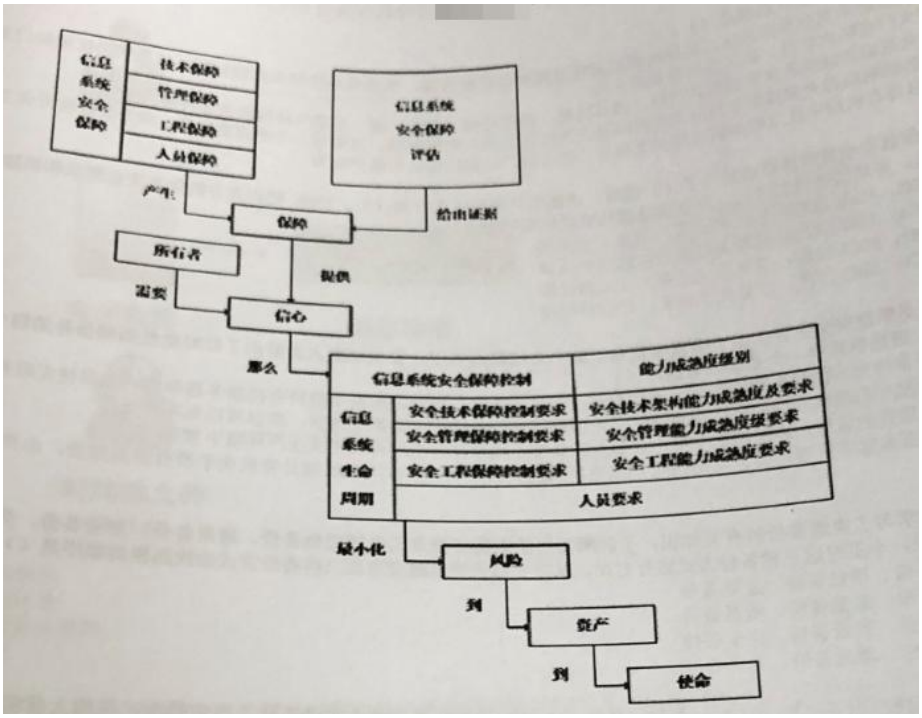
73. 以下哪个组织所属的行业的信息系统不属于关键信息基础设施？
A．人民解放军战略支援部队
B．中国移动吉林公司
C．重庆市公安局消防总队
D．上海市卫生与计划生育委员会

74. 目前应用面临的威胁越来越多，越来越难发现。对应用系统潜在的威胁目前还没有统一的分类，但小赵认为同事小李从对应用系统的攻击手段角度出发所列出的四项例子中有一项不对，请问是下面哪一项（）
A.数据访问权限 B.伪造身份 C.钓鱼攻击 D.远程渗透

75. 与 PDR 模型相比，P2DR 模型则更强调（）,即强调系统安全的（），并且以安全检测、（）和自适应填充“安全间隙“为循环来提高（）。
A．漏洞监测；控制和对抗；动态性；网络安全
B．动态性；控制和对抗；漏洞监测；网络安全
C．控制和对抗；漏洞监测；动态性；网络安全
D．控制和对抗；动态性；漏洞监测；网络安全

76. 某单位在进行内部安全评估时，安全员小张使用了单位采购的漏洞扫描软件进行单位内的信息系统漏洞扫描。漏洞扫描报告的结论为信息系统基本不存在明显的安全漏洞，然而此报告在内部审计时被质疑，原因在于小张使用的漏洞扫描软件采购于三年前，服务已经过期，漏洞库是半年前最后一次更新的。关于内部审计人员对这份报告的说法正确的是（）
A.内部审计人员的质疑是对的，由于没有更新漏洞库，因此这份漏洞扫描报告准确性无法保证
B.内部审计人员质疑是错的，漏洞扫描软件是正版采购，因此扫描结果是准确的
C．内部审计人员的质疑是正确的，因为漏洞扫描报告是软件提供，没有经过人为分析，因此结论不会准确
D.内部审计人员的质疑是错误的，漏洞软件是由专业的安全人员操作的，因此扫描结果是准确的

77. 信息系统安全保障评估概念和关系如图所示。信息系统安全保障评估，就是在信息系统所处的运行环境中对信息系统安全保障的具体工作和活动进行客观的评估。通过信息系统安全保障评估所搜集的（），向信息系统的所有相关方提供信息系统的（）能够实现其安全保障策略，能够将将其所面临的风险降低到其可接受的程度的主观信心。信息系统安全保障评估的评估对象是（），信息系统安全保障是一个动态持续的过程，涉及信息系统整个（），因此信息系统安全保障的评估也应该提供一种（）的信心。



A. 安全保障工作；客观证据；信息系统；生命周期；动态持续
B. 客观证据；安全保障工作；信息系统；生命周期；动态持续
C. 客观证据；安全保障工作；生命周期；信息系统；动态持续
D. 客观证据；安全保障工作；动态持续；信息系统；生命周期

78. 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

79. 组织应定期监控、审查、审计（）服务，确保协议中的信息安全条款和条件被遵守，信息安全事件和问题得到妥善管理。应将管理供应商关系的责任分配给指定的个人或（）团队。另外，组织应确保落实供应商符合性审查和相关协议要求强制执行的责任。应保存足够的技术技能和资源的可用性以监视协议要求尤其是（）要求的实现。当发现服务交付的不足时，宜采取（）.当供应商提供的服务，包括对（）方针、规程和控制措施的维持和改进等发生变更时，应在考虑到其对业务信息、系统、过程的重要性和重新评估风险的基础上管理。
A. 供应商；服务管理；信息安全；合适的措施；信息安全
B. 服务管理；供应商；信息安全；合适的措施；信息安全
C. 供应商；信息安全；服务管理；合适的措施；信息安全
D. 供应商；合适的措施；服务管理；信息安全；信息安全

80. 下列关于面向对象测试问题的说法中，不正确的是（）
A. 在面向对象软件测试时，设计每个类的测试用例时，不仅仅要考虑用各个成员方法的输入参数，还需要考虑如何设计调用的序列
B. 构造抽象类的驱动程序会比构造其他类的驱动程序复杂
C. 类 B 继承自类 A，如对 B 进行了严格的测试，就意味着不需再对类 A 进行测试
D. 在存在多态的情况下，为了达到较高的测试充分性，应对所有可能的绑定都进行测试

81. 火灾是机房日常运营中面临最多的安全威胁之一，火灾防护的工作是通过构建火灾预防、检测和响应系统，保护信息化相关人员和信息系统，将火灾导致的影响降低到可接受的程度。下列选项中，对火灾的预防、

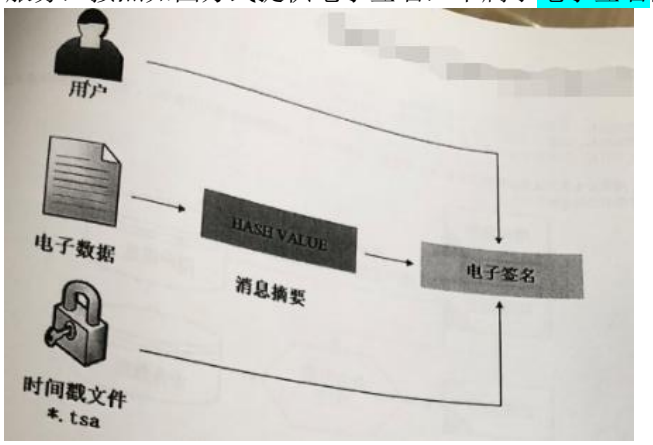
检测和抑制的措施描述错误的选项是（）。
A.将机房单独设置防火区，选址时远离易燃易爆物品存放区域，机房外墙使用非燃烧材料，进出机房区域的门采用防火门或防火卷帘，机房通风管设防火栓
B.火灾探测器的具体实现方式包括；烟雾检测、温度检测、火焰检测、可燃气体检测及多种检测复合等
C.自动响应的火灾抑制系统应考虑同时设立两组独立的火灾探测器，只要有一个探测器报警，就立即启动灭火工作
D.目前在机房中使用较多的气体灭火剂有二氧化碳、七氟丙烷、三氟甲烷等

82. 信息安全管理体系也采用了（） 模型，该模型可应用于所有的（）。ISMS 把相关方的信息安全要求和期望作为输入，并通过必要的()，产生满足这些要求和期望的（）。
A.ISMS；PDCA 过程；行动和过程；信息安全结果
B.PDCA;ISMS 过程；行动和过程；信息安全结果
C.ISMS;PDCA 过程；信息安全结果；行动和过程
D. PDCA;ISMS 过程；信息安全结果；行动和过程

83. 你是单位安全主管，由于微软刚发布了数个系统漏洞补丁，安全运维人员给出了针对此漏洞修补的四个建议方案，请选择其中一个最优方案执行（）
A.由于本次发布的数个漏洞都属于高危漏洞，为了避免安全风险，应对单位所有的服务器和客户端尽快安装补丁
B. 本次发布的漏洞目前尚未出现利用工具，因此不会对系统产生实质性危害，所以可以先不做处理
C. 对于重要的服务，应在测试环境中安装并确认补丁兼容性问题后再在正式生产环境中部署
D. 对于服务器等重要设备，立即使用系统更新功能安装这批补丁，用户终端计算机由于没有重要数据，由终端自行升级

84. 小王学习了灾备备份的有关知识，了解到常用的数据备份方式包括完全 备份、增量备份、差量备份，为了巩固所学知识，小王对这三种备份方式进行对比，其中在数据恢复速度方面三种备份方式由快到慢的顺序是（）
A.完全备份、增量备份、差量备份
B. 完全备份、差量备份、增量备份
C. 增量备份、差量备份、完全备份
D. 差量备份、增量备份、完全备份

85. 在网络交易发达的今天，贸易双方可以通过签署电子合同来保障自己的合法权益。某中心推出电子签名服务，按照如图方式提供电子签名，不属于电子签名的基本特性的是（）。



A. 不可伪造性 B.不可否认性
C.保证消息完整性 D.机密性

86. 风险评估文档是指在整个风险评估过程中产生的评估过程文档和评估结果文档，其中，明确评估的目的、职责、过程、相关的文档要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据的文档是（）

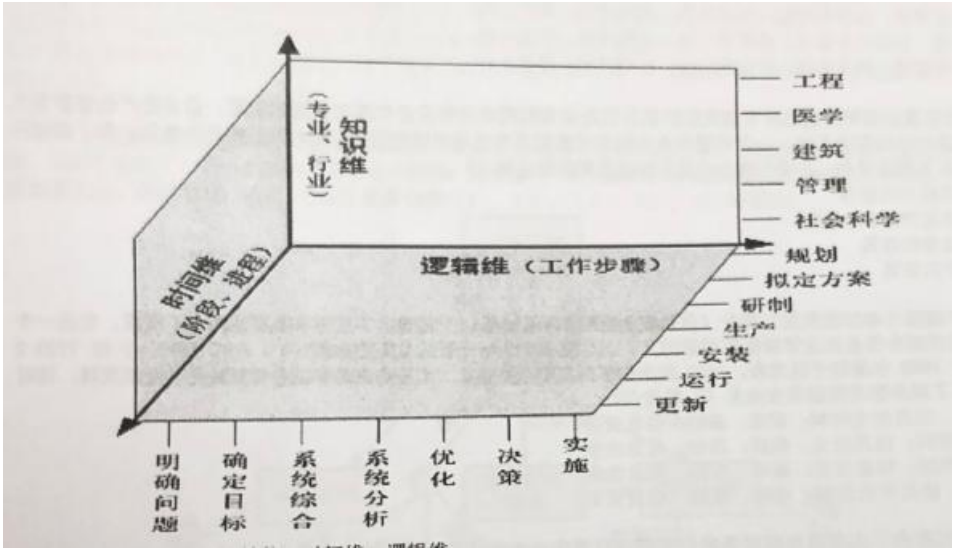
A《风险评估方案》 B.《风险评估程序》
C《资产识别清单》 D.《风险评估报告》

87. 等级保护实施根据 GB/T 25058-2010 《信息安全技术 信息系统安全等级保护实施指南》分为五大阶段；（）、总体规划、设计实施、（）和系统终止。但由于在开展等级保护试点工作时，大量信息系统已经建设完成，因此根据实际情况逐步形成了（）、备案、差距分析（也叫差距测评）、建设整改、验收测评、定期复查为流程的（）工作流程。和《等级保护实施指南》中规定的针对（）的五大阶段略有差异。
A. 运行维护；定级；定级；等级保护；信息系统生命周期
B. 定级；运行维护；定级；等级保护；信息系统生命周期
C. 定级运行维护；等级保护；定级；信息系统生命周期
D. 定级；信息系统生命周期；运行维护；定级；等级保护

88. 保护-检测-响应（Protection-Detection-Response,PDR）模型是（）工作中常用的模型，思想是承认（）中漏洞的存在，正视系统面临的（），通过采取适度防护、加强（）、落实对安全事件的响应、建立对威胁的防护来保障系统的安全。
A. 信息系统；信息安全保障；威胁；检测工作
B. 信息安全保障；信息系统；检测工作；威胁；检测工作
C. 信息安全保障；信息系统；威胁；检测工作
D. 信息安全保障；威胁；信息系统；检测工作

89. 在极限测试过程中，贯穿始终的是()
A.单元测试和集成测试
B.单元测试和系统测试
C.集成测试和验收测试
D.集成测试和系统测试
答案：单元测试，系统测试，验收测试，尤其包括单元和验收测试。

90. 美国系统工程专家霍尔（A.D.Hall）在 1969 年利用机构分析法提出著名的霍尔三维结构，使系统工程的工作阶段和步骤更为清晰明了，如图所示，霍尔三维结构是将系统工程整个活动过程分为前后紧密衔接的（）阶段和（）步骤，同时还考虑了为完全这些阶段和步骤所需要的各种（）。这样，就形成了由（）、（）、和知识维所组成的三维空间结构。



A. 五个；七个；专业知识和技能；时间维；逻辑维
B. 七个；七个；专业知识和技能；时间维；逻辑维
C. 七个；六个；专业知识和技能；时间维；逻辑维
D. 七个；六个；专业知识和技能；时间维；空间维

91. 社会工程学是（）与（）结合的学科，准确来说，它不是一门科学，因为它不能总是重复合成功，并且

在信息充分多的情况下它会失效。基于系统、体系、协议等技术体系缺陷的（），随着时间流逝最终都会失效，因为系统的漏洞可以弥补，体系的缺陷可能随着技术的发展完善或替代，社会工程学利用的是人性的“弱点”，而人性是（）,这使得它几乎是永远有效的（）。
A．网络安全；心理学；攻击方式；永恒存在的；攻击方式
B．网络安全；攻击方式；心理学；永恒存在的；攻击方式
C．网络安全；心理学；永恒存在的；攻击方式
D．网络安全；攻击方式；心理学；攻击方式；永恒存在的

92. 系统安全工程能力成熟度模型评估方法（SSAM, SSE-CMM Appraisal Method）是专门基于 SSE-CMM 的评估方法。它包含对系统安全工程-能力成熟度模型中定义的组织的（）流程能力和成熟度进行评估所需的（）。SSAM 评估过程分为四个阶段，（）、（）、（）、（）。
A．信息和方向；系统安全工程；规划；准备；现场；报告
B．信息和方向；系统工程；规划；准备；现场；报告
C．系统安全工程；信息；规划；准备；现场；报告
D．系统安全工程；信息和方向；规划；准备；现场；报告

93. 当使用移动设备时，应特别注意确保()不外泄。移动设备方针应考虑与非保护环境移动设备同时工作时的风险。当在公共场所、会议室和其他不受保护的区域使用移动计算设施时，要加以小心。应采取保护措施以避免通过这些设备存储和处理的信息未授权的访问或泄露，如使用()、强制使用秘钥身份验证信息。要对移动计算设施进行物理保护，以防被偷窃，例如，特别是遗留在汽车和其他形式的交通工具上、旅馆房间、会议中心和会议室。要为移动计算机设施的被窃或丢失等情况建立一个符号法律、保险和组织的其他安全要求的（）。携带重要、敏感和或关键业务信息的设备不宜无人值守，若有可能，要以物理的方式锁起来，或使用（）来保护设备。对于使用移动计算设施的人员要安排培训，以提高他们对这种工作方式导致的附加风险的意识，并且要实施控制措施。
A．加密技术；业务信息；特定规程；专用锁
B．业务信息；特定规程；加密技术；专用锁
C．业务信息；加密技术；特定规程；专用锁
D．业务信息；专用锁；加密技术；特定规程

94. 在规定的时间间隔或重大变化发生时，组织的额（）和实施方法（如信息安全的控制目标、控制措施、方针、过程和规程）应（）。独立评审宜由管理者启动，由独立被评审范围的人员执行，例如内部审核部、独立的管理人员或专门进行这种评审的第三方组织。从事这些评审的人员宜具备适当的（）。管理人员宜对自己职责范围内的信息处理是否符合合适的安全策略、标准和任何其他安全要求进行（）。为了日常功评审的效率，可以考虑使用自动测量和（）。评审结果和管理人员采取的纠正措施宜被记录，且这些记录宜予以维护。
A.信息安全管理；独立审查；报告工具；技能和经验；定期评审
B.信息安全管理；技能和经验；独立审查；定期评审；报告工具
C．独立审查；信息安全管理；技能和经验；定期评审；报告工具
D．信息安全管理；独立审查；技能和经验；定期评审；报告工具

95. 选择信息系统部署的场地应考虑组织机构对信息安全的需求并将安全性防在重要的位置，信息资产的保护很大程度上取决与场地的安全性，一个部署在高风险场所的额信息系统是很难有效的保障信息资产安全性的。为了保护环境安全，在下列选项中，公司在选址时最不应该选址的场地是().
A.自然灾害较少的城市
B．部署严格监控的独立园区
C．大型医院旁的建筑
D．加油站旁的建筑

96. 1998 年英国公布标准的第二部分《信安全管理体系规范》，规定（）管理体系要求与（）要求，它是一个组织的全面或部分信息安全管理体系评估的(),它可以作为一个正式认证方案的()。BS 7799-1 与 BS7799-2 经过修订于 1999 年重新予以发布，1999 版考虑了信息处理技术，尤其是在网络和通信领域应用的近期发展，同时还非常强调了商务涉及的信息安全及（）的责任。

A．信息安全；信息安全控制；根据；基础；信息安全
B．信息安全控制；信息安全；根据；基础；信息安全
C．信息安全控制；信息安全；基础；根据；信息安全
D．信息安全；信息安全控制；基础；根据；信息安全

97. 某计算机机房由于人员疏忽或设备老化可能会有发生火灾的风险。该计算机机房的资产价值为 200 万元；如果发生火灾，资产总值将损失至资产值的 25%；这种火灾发生的可能性为 25 年发生一次。则这种威胁的年度损失预期值为( ).
A．10,000 元 B.15,000 元 C.20,000 元 D.25,000 元

98. 安全审计师一种很常见的安全控制措施，它在信息全保障系统中，属于（）措施。
A．保护 B.检测 C.响应 D.恢复

99. 下列选项分别是四种常用的资产评估方法，哪个是目前采用最为广泛的资产评估方法（）。
A．基于知识的分析方法 B.基于模型的分析方法
C．定量分析 D.定性分析

100. 访问控制方法可分为自主访问控制、强制访问控制和基于角色访问控制，它们具有不同的特点和应用场景。如果需要选择一个访问控制模型，要求能够支持最小特权原则和职责分离原则，而且在不同的系统配置下可以具有不同的安全控制，那么在（1）自主访问控制，（2）强制访问控制，（3）基于角色的访问控制（4）基于规则的访问控制中，能够满足以上要求的选项有（）
A.只有（1）（2） B.只有（2）（3）
C.只有（3）（4） D.只有（4）