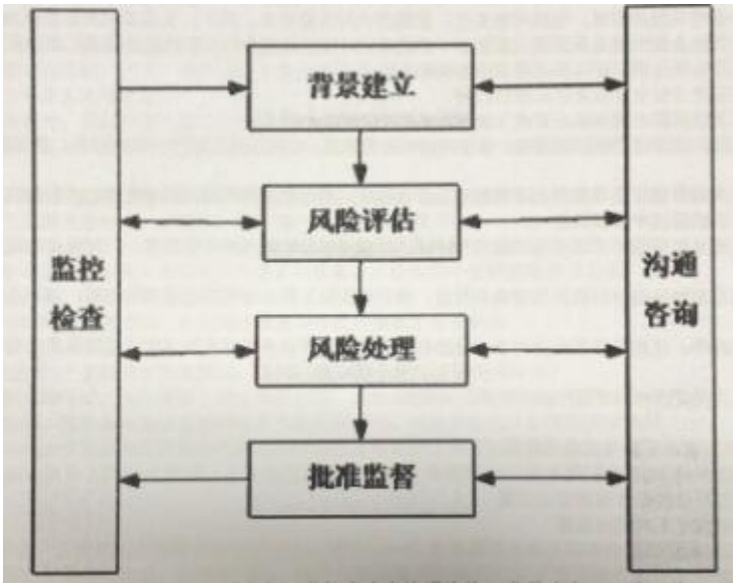
CISE 必须练习题

1.关于微软的 SDL 原则，弃用不安全的函数属于哪个阶段?
A.规划 B.设计 C.实现一 D.测试

2.优秀源代码审核工具具有哪些特点(　)
①安全性②多平台性③可扩展性④知识性⑤集成性
A. ①②③④⑤B.230C.①②③④D.②③

3.信息安全风险管理过程的模型如图所示。按照流程，请问，信息安全风险管理包括(　)六个方面的内容。(　)是信息安全风险管理的四个基本步骤，(　)则贯穿于这四个基本步骤中。



A. 背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询；背景建立、风险评估、风险处理和批准监督；监控审查和沟通咨询
B. 背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询；背景建立、风险评估、风险处理和监控审查；批准监督和沟通咨询
C. 背景建立、风险评估、风险处理、批准监督、监控审查和沟通咨询；背景建立、风险评估、风险处理和沟通咨询；监控审查和批准监督
D. 背景建立，风险评估、风险处理、批准监督、监控审查和沟通咨询：背景建立、风险评估、监控审查和批准监督；风险处理和沟通咨询

4.某公司在讨论如何确认已有的安全措施，对于确认已有安全措施，下列选项中描述不正确的是(　)
A.对有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施
B.安全措施主要有预防性、检测性和纠正性三种
C.安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁
D.对确认为不适当的安全措施可以置之不顾

5.密码是一种用来混滑的技术，使用者希望将正常的(可识别的)信息转变为无法识别的信息。但这种无法识信息部分是可以再加工并恢复和破解的，小刚是某公司新进的员工，公司要求他注册一个公司网站的账号，小刚使用一个安全一点的密码，请问以下选项中那个密码最安全（）
A.使用和与用户名相同的口令
B.选择可以在任何字典或语言中找到的口令
C.选择任何和个人信息有关的口令
D.采取数字，字母和特殊符号混合并且易于记忆

6.基于对（）的信任，当一个请求或命令来自一个“权威”人士时，这个请求就可能被毫不怀疑的（）。在（）中，攻击者伪装成“公安部门”人员，要求受害者转账到所谓的“安全账户”就是利用了受害者对权威的信任，在（）中，攻击者可能伪装成监管部门、信息系统管理人员等身份，去要求受害者执行操作，例如伪装成系统管理员，告诉用户请求配合进行一次系统测试，要求（）等。
A. 权威；执行；电信诈骗；网络攻击；更改密码
B. 权威；执行；网络攻击；电信诈骗；更改密码
C.执行；权威；电信诈骗；网络攻击；更改密码
D.执行；权威；网络攻击；电信诈骗；更改密码

7.在软件项目开发过程中，评估软件项目风险时，()与风险无关。
A. 高级管理人员是否正式承诺支持该项目
B. 开发人员和用户是否充分理解系统的需求
C. 最终用户是否同意部署已开发的系统
D. 升发需變的资金是否能按时到位

8.物理安全是一一个非常关键的领域，包括环境安全、设施安全与传输安全。其中，信息系统的设施作为直接存储、处理数据的载体，其安全性对信息系统至关重要。下列选项中，对设施安全的保障措施的描述正确的是（）
A. 安全区城不仅包含物理区域，还包含信息系统等软件区域
B. 建立安全区域需　要建立安全屏蔽及访问控制机制
C. 由于传统门镇容易被破解，因此禁止采用门锁的方式进行边界防护
D. 闭路电视监控系统的前端设备包括摄像机、数字式控制录像设备，后端设备包括中央控制设备、监视器等

9.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，而不应选择定性风险分析
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

10.与浏览器兼容性测试不需要考虑的问题是（）
A.　软件是否可以在不同的 J2EE 中运行
B.不同的浏览器是否可以提供合适的安全设置
B.　脚本和插件是否适用于不同的浏览器
D.符合最新 HIML 版本的页面能否在浏览器中正确显示

11.下列关于测试方法的叙述中不正确的是()
A.从某种角度上讲，白盘测试与黑盒测试都属于动态测试
B.功能测试属于黑盒测试
C.结构测试属于白盒测试
D.对功能的测试通常是要考虑程序的内部结构的

12,小王学习了灾难备份的有关知识,了解到常用的数据备份方式包括完全备份、增最备份、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.完全各份、差量备份、增量备份
C.增量备份、差量各份、完全备份
D.差量备份、增量备份、完全备份

13.以下哪一项不属于 Web 应用软件表示层测试关注的范畴( )
A.排版结构的测试
B 数据完整性测试
C.客户端兼容性的测试
D.链接结构的测试

14.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-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

15.以下哪些不是《国家网络空间安全战略》中阐述的我国网络空间当前任务？
A.捍卫网络空间主权
B.保护关键信息基础设施
C.提升网络空间防护能力
D 阻断与国外网络连接

16.在信息安全保障工作中，人才是非常重要的因素，近年来，我国一直高度重视我国信息安全人才队伍的培养建设。在以下关于我国关于人才培养工作的描述中，错误的是(　)。
A.在《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003])

27 号)中，针对信息安全人才建设与培养工作提出了“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
B.2015 年，为加快网络空间安全高层次人才培养，经报国务院学位委员会批准，国务院学位委员会、教育部决定在“工学”门类下增设“网络空间安全”一级学科，这对于我国网络信息安全人才成体系化、规模化、系统化培到积极的推动作用
C 经过十余年的发展，我国信息安全人才培养已经成熟和体系化，每年培养的信息安全从业人员的数量较多，能同社会实际需求相匹配；同时，高校信息安全专业毕业人才的综合能力要求高、知识更全面，因而社会化培养重点放在非安全专业人才培养上
D.除正规大学教育外，我国信息安全非学历教育已基本形成了以各种认证为核心，辅以各种职业技能培训的信息安全人才培训体系，包括“注册信息安全专业人员(CISP) ”资质认证和一些大型企业的信息安全资质认证

17.王明买了一个新的蓝牙耳机，但王明听说使用蓝牙设备有一定的安全威胁，于是王明找到对蓝牙技术有所了解的王红，希望王红能够给自己一.点建议，以下哪一条建议不可取( )
A. 在选择使用蓝牙设备时，应考虑设备的技术实现及设置是否具备防止上述安全威胁的能力 B.选择使用功能合适的设备面不是功能尽可能多的设备、尽量关闭不使用的服务及功能
B. C 如果蓝牙设备丢失，最好不要做任何操作
D.在配对时使用随机生成的密钥、不使用时设置不可被其他蓝牙设备发现

18.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(DRP)文档

19. Hadop 是目前广泛应用的大数据处理分析平台。在 Hadoop1. 0. 0 版本之前，Hadoop 并不存在安全认证一说。认集群内所有的节点都是可靠的，值得信赖的。用户与服务器进行交互时并不需要进行验证。导致存在恶意用户伪装成真正的用户或者服务器入侵到 Hadoop 集群上，恶意的提交作业，篡改分布式存储的数据，伪装成 NameNo 或者 TaskTracker 接受任务等。在 Hadoop2.0 中引入了 Kerberos 机制来解决用户到服务器的认证问题，Kerber 的认证过程不包括( )
A. 获得票据许可票据
B. 获得服务许可票据
C. 获得密钥分配中心的管理权限
D. 获得服务

20. 下面哪个阶段不属于软件的开发时期( )

A.详细设计
B 总体设计
C 编码
D.需求分析

21. 下列关于软件需求管理与需求开发的论述正确的是(　　)
A.所谓需求管理，是指对需求开发的管理
B.需求管理包括：需求获取、需求分析、需求定义和需求验证
C.需求开发是将用户需求转换为应用系统成果的过程
D.在需求管理中，要求维持对原有需求和所有产品需求的双向跟踪

22.信息安全是通过实施一组合适的(　　)而达到的，包括策略、过程、规程、(　)以及软件和硬件功能。在必要时需建立、实施、监视、评审和改进包含这些控制措施的（　）过程，以确保满足该组织的特定安全和(　　）。这个过程　宜与其他业务(　　)联合进行。
A 信息安全管理；控制措施；　组织结构；业务目标；管理过程
B.组织结构；控制措施；信息全管理；业务目标；管理过程
C 控制措施；:组织结构；信息安全管理；业务目标；管理过程
D.控制措施；组织结构；业务目标；信息安全管理；管理过程

23.了解社会工程学攻击是应对和防御（　　）的关键，　对于信息系统的管理人员和用户，都应该了解社会工程学攻击的概念和攻击的（　　）。组织机构可采取对相关人员实施社会工程学培训来帮助员工了解什么是社会工程学攻击，如何判断是否存在社会工程学攻击，这样才能更好地保护信息系统和（　）。因为如果对攻击方式有所了解，那么识破攻击者的伪装就（　）。因此组织应持续不断的向员工提供安全意识的培训和教育，向员工灌输（　），从而降低社会工程学攻击的风险。
A.社会工程学攻击；越容易；原理；个人数据；安全意识
B.社会工程学攻击；原理；越容易；个人数据；安全意识
C.原理；社会工程学攻击；个人数据；越容易；安全意识
D.社会工程学攻击；原理；个人数据；越容易；安全意识

24. 某 IT 公司针对信息安全事件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的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、更新现有应急预案五个阶段，流程完善可用
C. 公司应急预案包括了基础环境类、业务系统类、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 一 2007 《信息安全技术信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.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要求较高的系统，强制访间控制模型有多种类型，如 BLP、Biba、Clark-illson 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 种对 BLP 模型的描述中，正确的是(　　)。

A. BLP 模型用于保证系统信息的完整性

B. BLP 模型的规则是“向下读，向上写”

C. BLP 的自主安全策略中，系统通过比较主体与客体的访问类属性控制主体对客体的访问

D. BUP 的强制安全策略使用一个访问控制矩阵表示

25. 对操作系统软件安装方面应建立安装(　)，运行系统要仅安装经过批准的可执行代码，不安装开发代码和(　)，应用和操作系统软件要在大范围的、成功的测试之后才能实施。而且要仅由受过培训的管理员，根据合适的(　)，进行运行软件、应用和程序库的更新；必要时在管理者批准的情况下，仅为了支持目的，才授予供应商物理或迎辑访问权，并且要监督供应商的活动。对于用户能安装何种类型的软件，组织宜定义并强制执行严格的方针，宜使用(　　)。不受控制的计算机设备上的软件安装可能导致脆弱性，进而导致信息泄露；整体性损失或其他信息安全事件或违反(　　)。

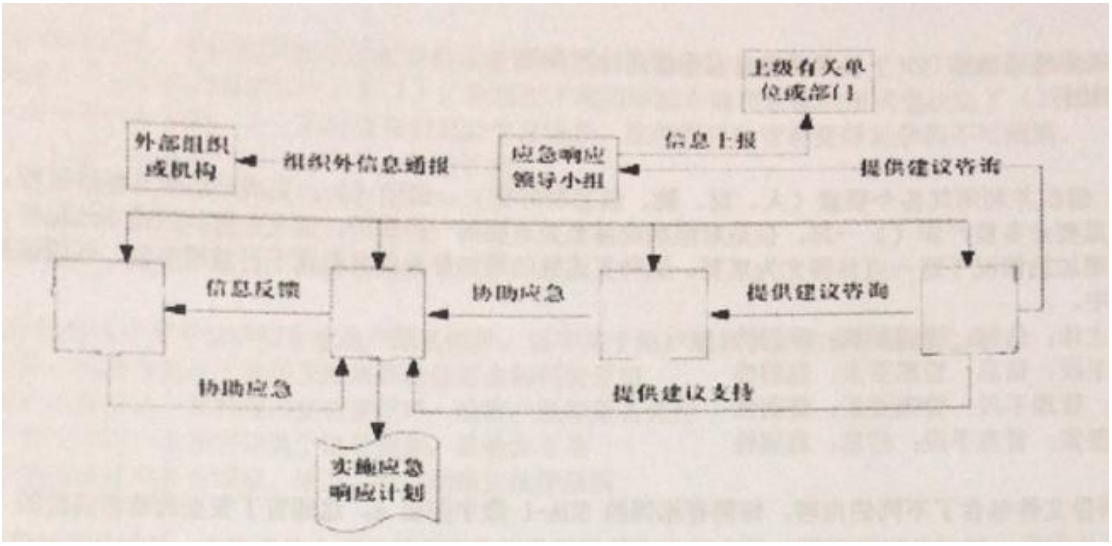
A 控制规程；编译程序；管理授权；最小特权方针；知识产权

B 编译程序；控制规程；管理授权；最小特权方针；知识产权

C.控制规程；管理授权；编译程序；最小特权方针；知识产权

D.控制规程；最小特权方针；编译程序；管理授权；知识产权

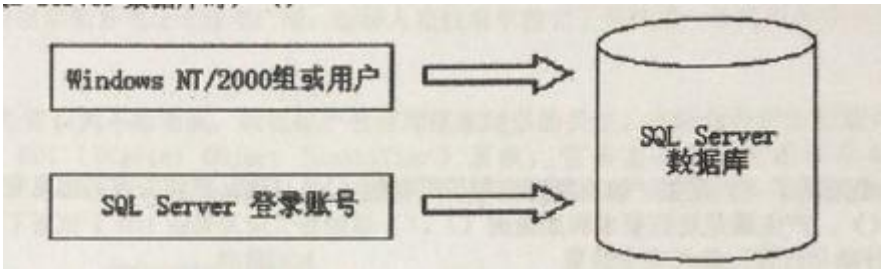
27.网络与信息安全应急预案是在分析网络与信息系统突发事件后果和应急能力的基础上，针对可能发生的重大网络与信息系统突发事件，预先制定的行动计划或应急对策。应急预案的实施需要各子系统的相互配合与协调　下面应急响应工作流程图中，空白方框中从右到左依次填入的是（　　）。



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

28. SQLServer 支持两种身份验证模式，即 Windows 身份验证模式和混合模式。SQL Server 的混合模式是指，当网络用户尝试连接到 SQL Server 数据库时，(　　)



A. Windows 获取用户输入的用户和密码，并提交给 SQL Server 进行身份验证，并决定用户的数据库访问权限；
B. B. SQL Server 根据用户输入的用户和密码，提交给 Windows 进行身份验证，并决定用户的数据库访问权限；
C. SQL Server 根据已在 Windows 网络中登录的用户的网络安全属性，对用户身份进行验证，并决定用户的数据访权限；
D.登录到本地 Windows 的用户均可无限制访问 SQL Server 数据库。

29.物联网将我们带入一个复杂多元、综合交互的新信息时代，物联网安全成为关系国计民生的大事，直接影响寸个人生活和社会稳定。物联网安全问题必须引起高度重视，并从技术、标准和法律方面予以保障。物联网的感知安全技术主要包括(　)、(　) 等。实现 RFID 安全性机制所采用的方法主要有三类，(　)、(　) 和(　)。传感器络认证技术主要包含(　)、(　) 和(　)。
A. RFID 安全技术；传感器网络安全技术；;内部变体认证、网络与用户认证，以及广插认证；物理机制、密码机制，以及二者相结合的方法
B. RFID 安全技术；传感器技术；物理机制、密码机制，以及二者相结合的方法实体认证、网络与用户认证，以广播认证
C. RFID 安全技术:传感器网络安全技术；物理机制、密码机制，以及二者相结合的方法；内部实体认证、网络与户认证，以及广播认证
D.RFID 技术；传感器技术； 物理机制、密码机制，以及二者相结合的方法；实体认证、网络与用户认证，以及广播认证

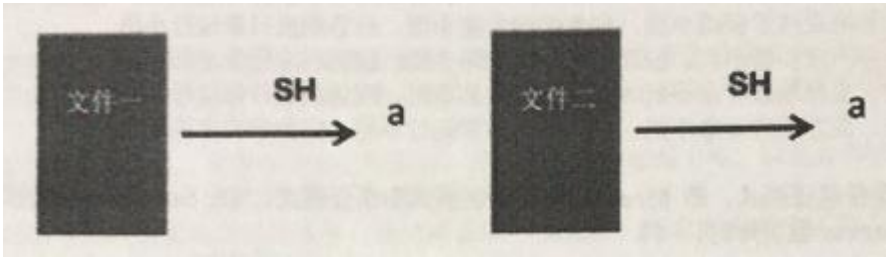
30.建立并完善(　)是有效应对社会工程学攻击的方法，通过(　　)的建立，使得信息系统用户需要遵循(　　)来实某些操作，从而在一定程度上降低社会工程学的影响。例如对于用户密码的修改，由于相应管理制度的要求，(　　)需要对用户身价进行电话回拨确认才能执行，那么来自外部的攻击者就可能很难伪装成为内部工作人员来进(　　)，因为他还需要想办法拥有一个组织机构内部电话才能实施。
A 信息安全管理体系；安全管理制度；规范；网络管理员；社会工程学攻击

B.信息安全管理体系，安全管理制度；网络管理员；规范；社会工程学攻击
C.安全管理制度；信息安全管理体系；规范； 网络管理员；社会工程学攻击
D.信息安全管理体系；网络管理员；安全管理制度；规范；社会工程学攻击

31 怎样安全上网不中毒，现在是网络时代了，上网是每个人都会做的事，但网络病毒一直是比较头疼的， 电脑中毒也比较麻烦。某员工为了防止在上网时中毒，使用了影子系统，他认为恶意代码会通过以下方式传播，但有一项是安全的，请问是(　　)。
A.网页挂马
B.利用即时通讯的关系链或伪装 P2P 下载资源等方式传播到目标系统中
C. Google 认证过的插件
D. 垃圾邮件

32.管理，是指(　　)组织并利用其各个要素(人、财、物信息和时空)，借助(　　)，完成该组织目标的过程，其中，(　　)就像其他重要业务资产和(　　)一样，也是对组织业务至关重要的一种资产，因此需要加以适当地保护。在业务环境互连日益增加的情况下这一点显得尤为重要。 这种互连性的增加导致信息暴露于日益增多的、范围越来越广的威胁和(　　)当中。
A.管理手段；管理主体；信息；管理要素；脆弱性
B.管理主体；管理手段信息；管理要素；脆弱性
C.管理主体；信息；管理手段；管理要素；脆弱性
D.管理主体；管理要素；管理手段；信息；脆弱性

33 如下图所示，两份文件包含了不同的内容， 却拥有相同的 SIHA 1 数字签名 a，这违背了安全的哈希函数的(　　)性质。



A.单向性
B 弱抗碰撞性
C.强抗碰撞性
D.机密性

34. 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

35.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：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

36.下列选项中，对物理与环境安全的描述出现错误的是(　)。
A. 物理安全确保了系统在对信息进行采集、传输、存储、处理等过程中的安全
B. 物理安全面对的是环境风险及不可预知的人类活动，是一个非常关键的领域
C. 物理安全包括环境安全、系统安全、设施安全等
D. 影响物理安全的因素不仅包含自然因素，还包含人为因素

37.风险处理是依据(　)，选择和实施合适的安全措施。风险处理的目的是为了将(　)始终控制在可接受的范围内。风险处理的方式主要有(　)、(　)、(　) 和(　)四种方式。
A.　风险；风险评估的结果；降低；规避；转移；接受
B.　风险评估的结果；风险；降低；规避；转移；接受
C.　风险评估；风险；降低；规避；转移；接受
D.　风险；风险评估；降低；规避；转移；按受

38.信息收集是(　)攻击实施的基础，因此攻击者在实施前会对目标进行(　)，了解目标所有相关的(　)。这些资料和信息对很多组织机构来说都是公开或者看似无用的，然而对攻击者来说，这些信息都是非常有价值的，这些信息收集得越多，离他们成功得实现(　)就越近。如果认为信息没有价值或者价值非常低，组织机构通常不会采取措施(　)，这正是社会工程学攻击者所希望的。
A.信息收集；社会工程学；资料和信息；身份伪装；进行保护
B 社会工程学；信息收集；资料和信息；身份伪装；进行保护
C.社会工程学；信息收集；身份伪装；资料和信息；进行保护
D.信息收集；资料和信息；社会工程学；身份伪装；:进行保护

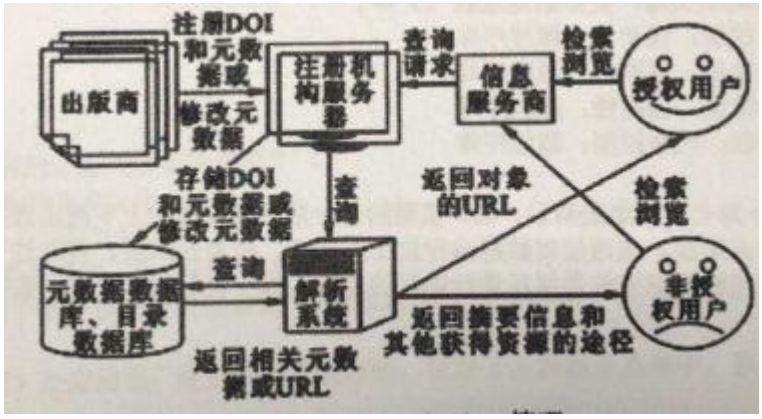
39. 信息是流动的，在信息的流动过程中必须能够识别所有可能途径的(　)与(　)；而对于信息本身而言，信息的敏感性的定义是对信息保护的(　)和(　)，信息在不同的环境存储和表现的形式也决定了(　)的效果，不同的载体下，可能体现出信息的(　)、临时性和信息的交互场景，这使得风险管理变得复杂和不可预测。
A.　基础；依据；载体；环境；永久性；风险管理
B.　基础；依据；载体；环境；风险管理；永久性
C.　载体；环境；风险管理；永久性；基础；依据
D.　载体；环境；基础；依据；风险管理；永久性

40. 软件安全设计和开发中应考虑用户隐私保护，以下关于用户隐私保护的说法错误的是?

A.告诉用户需要收集什么数据及搜集到的数据会如何被使用
B.当用户的数据由于某种原因要被使用时，给客户选择是否允许
C.用户提交的用户名和密码属于隐私数据，其他都不是
D.确保数据的使用符合国家、地方、行业的相关法律法规

41.随着时代的发展，有很多伟人都为通信事业的发展贡献出自己力量，根据常识可知以下哪项是正确的(　　)
A.19 世纪中叶以后，随着电磁技术的发展，诞生了笔记本电脑，通信领域产生了根本性的飞跃，开始了人类通信新时代
B.1837 年，美国人费曼发明了电报机，可将信息转换成电脉冲传向目的地，再转换为原来的信息，从而实现了长途电报通信
C.1875 年，贝尔(Bell)发明了电话机。1878 年在相距 300 公里的波士顿和纽约之间进行了首次长途电话实验，获得了成功
D. 1906 年美国物理学家摩斯发明出无线电广播。法国人克拉维尔建立了英法第一条商用无线电线路，推动了无线电技术的进一步发展

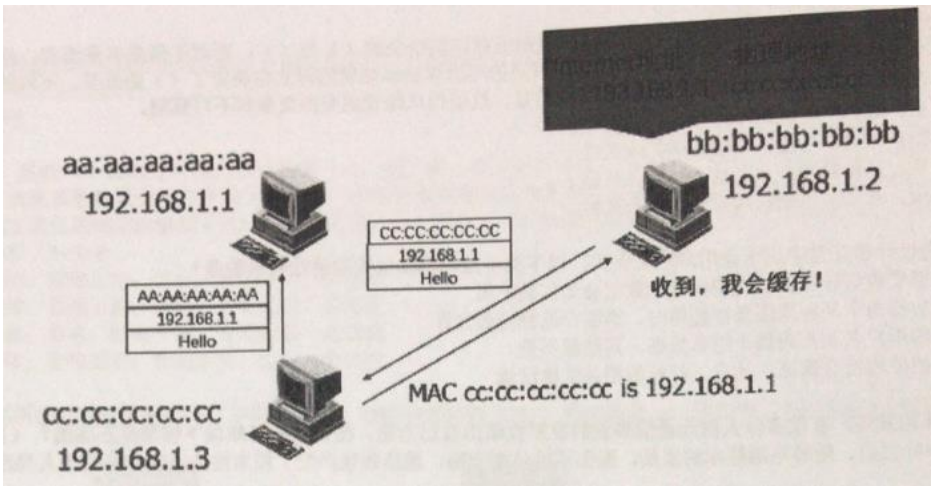
42.随着人们信息安全意识的不断增强，版权保护也受到越来越多的关注。在版权保护方面国内外使用较为广泛的是数字对象标识符 DOI（Digital Object Identifier)系统,它是由非赢利性组织国际 DOI 基金会 IDF(International DOI Foundation） 研究设计的，在数字环境下标识知识产权对象的一种开放性系统。DOI 系统工作流程如图所示，则下面对于 DOI 系统认识正确的是(　　)



A. DOI 是一个暂时性的标识号，由 International DOI Foundation 管理
B. DOI 的优点有唯一性、持久性、兼容性、或操作性、动态更新
C. DOI 命名规则中前缀和后级两部之间用“;”分开
D. DOI 的体现形式只有网络域名和字符码两种形式

43. 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

44.攻击者通过向网络或目标主机发送伪造的 ARP 应答报文，修改目标计算机上 ARP 缓存，形成一个错误的 IP 地<->MAC 地址映射，这个错误的映射在目标主机在需要发送数据时封装错误的 MAC 地址。欺骗攻击过程如下图示，其属于欺骗攻击中的哪一种欺骗攻击的过程( )

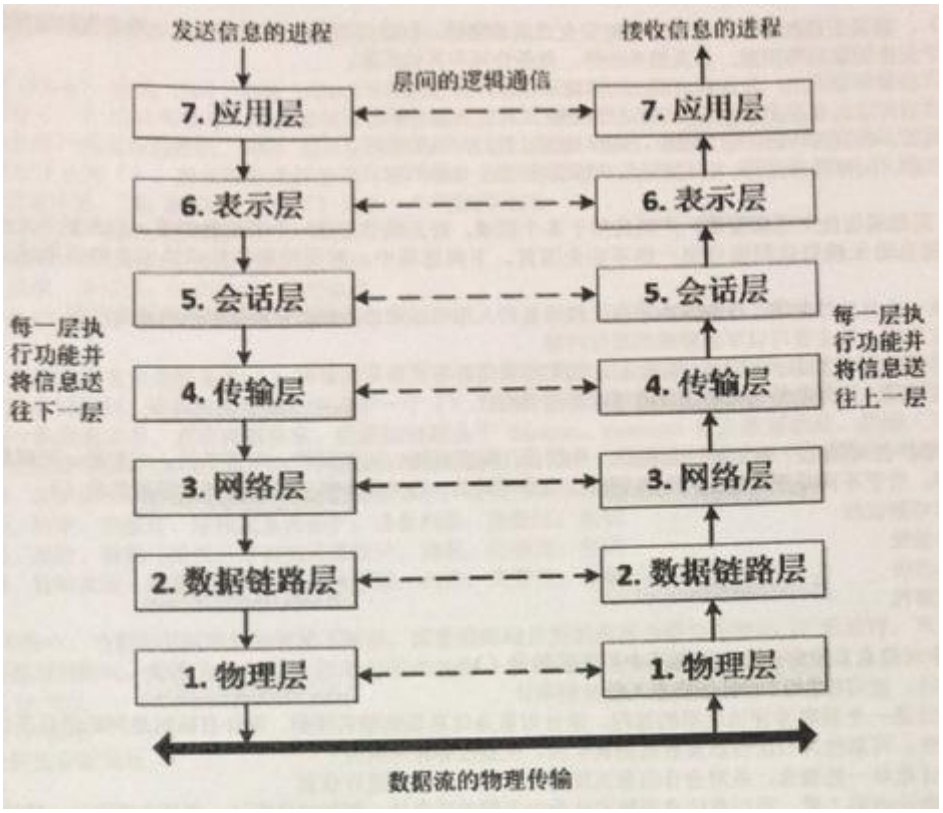


A. ARP
B. IP
C. DNS
D. SN

45. 组织应依照已确定的访同控制策略限制对信息和( )功能的访问。对访问的限制要基于各个业务应用要求，访问控制策略还要与组织的访问策略一致。应建立安全登录规程控制实现对系统和应用的访间。宜选择合适的身份验证技术以验证用户身份。在需要强认证和( )时，宜使用如加密、智能卡、令牌或生物手段等替代密码的身份验证方法。应建立交互式的口令管理系统，并确保使用优质的口令。对于可能覆盖系统和应用的控制措施的实用工具用程序的使用，应加以限制并( )。对程序源代码和相关事项(例如设计、说明书、验证计划和确认计划)的访问生严格控制，以防引入非授权功能、避免无意识的变更和维持有价值的知识产权的( )。对于程序源代码的保存，以通过这种代码的中央存储控制来实现，更好的是放在( )中。

A. 应用系统；身份验证；严格控制；保密性；源程序库
B. 身份验证；应用系统；严格控制；保密性；源程序库
C. 应用系统；严格控制；身份验证；保密性；源程序库
D. 应用系统；保密性；身份验证；严格控制；源程序库

46. OSI 模型把网络通信工作分为七层，如图所示，OSI 模型的每一层只与相邻的上下两层直接通信，当发送进程需要发送信息时，它把数据交给应用层。应用层对数据进行加工处理后，传给表示层。再经过一次加工后，数据被送到会话层。这一过程一直继续到物理层接收数据后进行实际的传输，每一次的加工又称为数据封装。其中 IP 层对应 OSI 模型中的那一层( )



A.应用层　B.传输层　C.应用层　D.网络层

47.以下关于软件安全问题对应关系错误的是?（　）
A.缺点(Defect)一软件实现和设计上的弱点
B.缺陷(Bug)一实现级上的软件问题
C.瑕疵(Flaw) 一种更深层次、设计层面的的问题
D.故障(Failure) 一由于软件存在缺点造成的一 种外部表现，是静态的、程序执行过程中出现的行为表现

48.自主访问控制(DAC) 是应用很广泛的访问控制方法，常用于多种商业系统中。以下对 DAC 模型的理解中，存在错误的是(　)。
A.在 DAC 模型中，资源的所有者可以规定谁有权访问它们的资源
B. DAC 是一种对单个用户执行访问控制的过程和措施
C. DAC 可为用户提供灵活调整的安全策略，具有较好的易用性和可扩展性，可以抵御特洛伊木马的攻击
D.在 DAC 中，具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体

49. 恶意代码经过 20 多年的发展，破坏性、种类和感染性都得到增强。随着计算机的网络化程度逐步提高，网络传播恶意代码对人们日常生活影响越来越大。小李发现在自己的电脑查出病毒的过程中，防病毒软件通过对有毒 件的检测，将软件行为与恶意代码行为模型进行匹配，判断出该软件存在恶意代码，这种方式属于(　)
A.简单运行　B.行为检测　C.是特征数据匹配　D.特征码扫描

50.信息安全风险值应该是以下哪些因素的函数?（ ）
A 信息资产的价值、面临的威胁以及自身存在的脆弱性
B.病毒、黑客、漏洞等
C.保密信息如国家秘密、商业秘密等
D.网络、系统、应用的复杂程度

51.管理层应该表现对（ ），程序和控制措施的支持，并以身作则。管理职责要确保雇员和承包方人员都了解（ ）角色和职责，并遵守相应的条款和条件。组织要建立信息安全意识计划，并定期组织信息安全（ ）。组织 立正式的（ ），确保正确和公平的对持被怀疑安全违规的雇员。纪律处理过程要规定（ ），考虑例如违规的性质、重要性及对于业务的影响等因素，以及相关法律、业务合同和其他因素。
A.信息安全；信息安全政策；教育和培训；纪律处理过程；分级的响应
B 信息安全政策；信息安全；教育和培训；纪律处理过程；分级的响应
C.信息安全政策；教育和培训；信息安全；纪律处理过程分级的响应
D.信息安全政策；纪律处理过程；信息安全；教育和培训；分级的响应

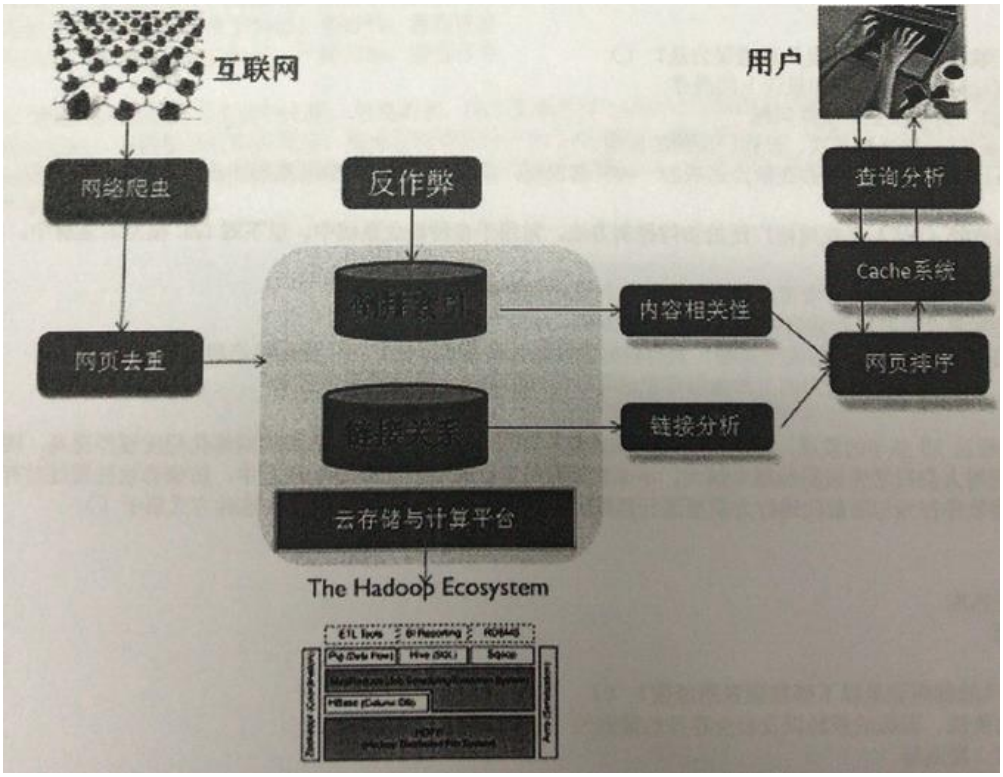
52.近几年，无线通信技术迅猛发展，广泛应用于各个领域。而无线信道是一一个开放性信道,它在赋予无线用户通信自由的同时也给无线通信网络带来一些不安全因素。下列选项中，对无线通信技术的安全特点描述正确的是
A 无线信道是一个开放性信道，任何具有适当无线设备的人均可以通过搭线窃听而获得网络通信内容
B 通过传输流分析，攻击者可以掌握精确的通信内容
C.对于无线局城网络和无线个人区域网络来说，它们的通信内容更容易被窃听
D.群通信方式可以防止网络外部人员获取网络内部通信内容

53.软件的可维护性可用七个质量特性来衡量，分别是:可理解性、可测试性、可修改性、可靠性、可移植性、可使用性和效率。对于不同类型的维护，这些侧重点也是不同的。在可维护性的特性中相互促进的是
A.可理解性和可测试性
B.效率和可移植性
C.效率和可修改性
D.效率和可理解性

54. 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 信息系统审计是单一的概念， 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

55.随着互联网的迅猛发展、WEB 信息的增加，用户要在信息海洋里查找自己所

需的信息，就象大海捞针一样，搜索引擎技术恰好解决了这难题。以下关于搜索引擎技术特点的描述中错误的是(　　)



A.搜索引擎以一定的策略在 Web 系统中搜索和发现信息

B.搜索引擎可以分为目录导航式与网页索引式

C.搜索器在 Internet 上逐个访问 Web 站点。并建立一个网站的关键字列表索引器功能是理解搜索器获取的信息向用户显示查询结果

D.索引器功能是理解搜索器获取的信息，向用户显示查询结果

56. “规划(Plan)实施 (Do)一检查(Check) 一处置(Aet)” (PDCA 过程)又叫(　　)，是管理学中的一个通用模型，最早由(　　)于 1930 年构想，后来被美国质量管理专家(　　)博士在 1950 年再度挖掘出来，并加以广泛宣传和运用于持续改善产品质量的过程。PDCA 循环就是按照“规划、实施、检查、处置”的顺序进行质量管理，并且循环不止地进行下去的(　　)，建立符合国际标准 ISO 9001 的质量管理体系即是一个典型的 POCA 过程，建立 ISO14001 环境管理体系、ISO 20000IT 服务(　　)也是一个类似的过程。

A.质量环；休哈特；戴明；管理体系；科学程序

B.质量环；戴明；休哈特；管理体系；科学程序

C 质量环；戴明；休哈特；科学程序；管理体系

D 质量环；休哈特；戴明；科学程序；管理体系

57. ZigBee 主要的信息安全服务为(　　)、(　　)、(　　)、(　　)。访问控制使设备能够选择其愿意与之通信的其他设备。为了实现访问控制，设备必须在 ACL 中维护一个(　　)，表明它愿意接受来自这些设备的数据。数据加密使用的密钥可能是一组设备共享，或者两两共享。数据加密服务于 Beacon、command 以及

数据载荷。数据(　)主要是利用消息完整性校验码保证没有密钥的节点不会修改传输中的消息，进一步确认消息来自一个知道(　)的节点。
A 访问控制、数据加密、数据完整性、序列抗重播保护；设备列表；完整性；密钥
B.访问控制、加密、完整性、序列抗重播保护；设备列表；完整性；密钥
C.访问控制、加密、数据完整性、序列抗重播保护；列表；完整性；密钥
D.访问控制、数据加密、数据完整性、序列抗重播；列表；完整性；密钥

58.在一个网络中，当拥有的网络地址容量不够多，或普通终端计算机没有必要分配静态 IP 地址时，可以采用通过在计算机连接到网络时，每次为其临时在 IP 地址池中选择一个 IP 地址并分配的方式为(　)
A 动态分配 IP 地址
B.静态分配 IP 地址
C.网络地址转换分配地址
D.手动分配

59.信息安全风险管理是基于(　)的信息安全管理，也就是，始终以(　)为主线进行信息安全的管理。应根据实际(　)的不同来理解信息安全风险管理的侧重点，即(　)选择的范围和对象重点应有所不同。
A 风险；风险；信息系统；风险管理
B.风险；风险；风险管理；信息系统
C.风险管理；信息系统；风险；风险
D.风险管理；风险；风险；信息系统

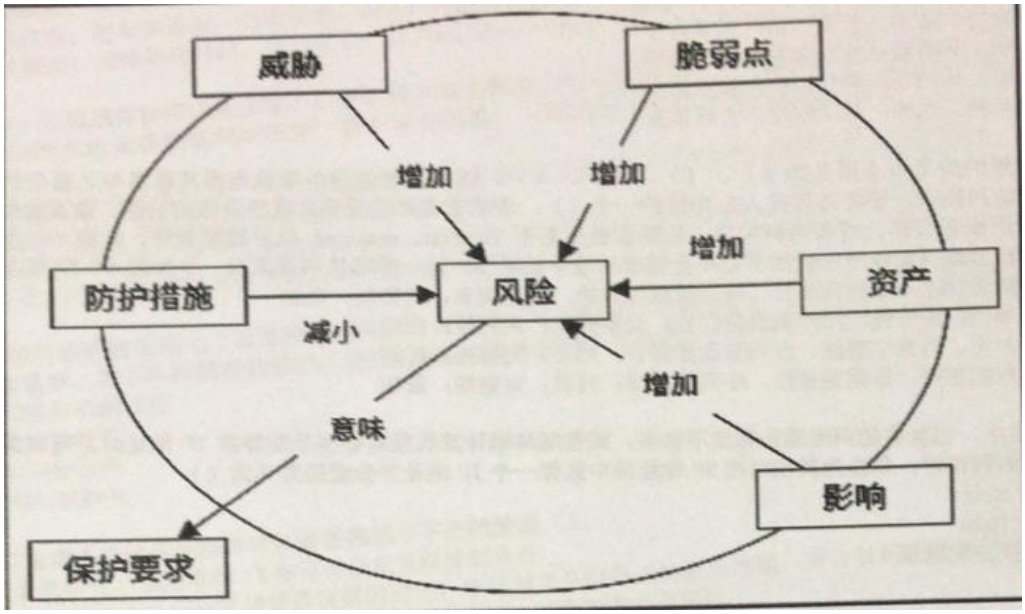
60.某商贸公司信息安全管理员考虑到信息系统对业务影响越来越重要，计划编制本单位信息安全应急响应预案，在向主管领导写报告时，他列举了编制信息安全应急响应预案的好处和重要性，在他罗列的四条理由中，其中不适合作为理由的一条是(　)
A.应急预案是明确关键业务系统信息安全应急响应指挥体系和工作机制的重要方式
B.应急预案是提高应对网络和信息系统突发事件能力，减少突发事件造成的损失和危害，保障信息系统运行平稳、安全、有序、高效的手段
C.编制应急预案是国家网络安全法对所有单位的强制要求，因此必须建设
D.应急预案是保障单位业务系统信息安全的重要措施

61.数据链路层负责监督相邻网络节点的信息流动，用检错或纠错技术来确保正确的传输，确保解决该层的流量控制问题。数据链路层的数据单元是(　　)
A.报文 B.比特流 C.帧 D.包

62.以下对于标准化特点的描述哪项是错误的?
A.标准化的对象是共同的、可重复的事物。不是孤立的一件事、一个事物
B.标准化必须是静态的，相对科技的进步和社会的发展不能发现变化
C.标准化的相对性，原有标准随着社会发展和环境变化，需要更新
D.标准化的效益，通过应用体现经济和社会效益，否则就没必要

63. 以下哪个是国际信息安全标准化组织的简称?
A. ANSI
B. ISO
C. IEEE
D. NIST

64.风险，在 GB/T 22081 中定义为事态的概率及其结果的组合。风险的目标可能有很多不同的方面，如财务目标，健康和人身安全目标、信息安全目标和环境目标等；目标也可能有不同的级别，如战略目标、组织目标、项目目标、产品目标和过程目标等。ISO/IEC 13335-中揭示了风险各要素关系模型，如图所示。请结合此图，怎么才能降低风险对组织产生的影响？



A 组织应该根据风险建立响应的保护要求，通过构架防护措施降低风险对组织产生的影响
B.加强防护措施，降低风险
C.减少威胁和脆弱点降低风险
D.减少资产降低风险

65.某公司财务服务器受到攻击被攻击者删除了所有用户数据，包括系统日志，公司网络管理员在了解情况后，给出了一些解决措施建议，作为信息安全主管，你必须指出不恰当的操作并阻止此次操作( )
A.由于单位并无专业网络安全应急人员，网络管理员希望出具授权书委托某网络安全公司技术人员对本次攻击进行取证
B.由于公司缺乏备用硬盘，因此计划将恢复服务器上被删除的日志文件进行本地恢复后再提取出来进行取证
C.由于公司缺乏备用硬盘，因此网络管理员申请采购与服务器硬盘同一型号的硬盘用于存储恢复出来的数据
D 由于公司并无专业网络安全应急人员，因此由网络管理员负责此次事件的应急协调相关工作

66.在你对远端计算机进行 ping 操作，不同操作系统回应的数据包中初始 TIL 值是不同的，TTL 是 IP 协议包中的一个值，它告诉网络，数据包在网络中的时间是否太长而应被丢弃。(简而言之，你可以通过 TTL 值推算一下下列数据包已经通过了多少个路由器)根据回应的数据包中的 TTL 值，可以大致判断(　　)
A.内存容量
B.操作系统的类型
C.对方物理位置
D.对方的 MAC 地址

67. （ ）攻击是建立在人性“弱点”利用基础上的攻击，大部分的社会工程学攻击都是经过( )才能实施成功的。即使是最简单的“直接攻击”也需要进行( )。如果希望受害者接受攻击者所( )，攻击者就必须具备这个身份所需要的( )。
A 社会工程学；精心策划；前期的准备；伪装的身份；一些特征
B.精心策划；社会工程学；前期的准备；伪装的身份:一些特征
C.精心策划；社会工程学；伪装的身份；前期的准备；一些特征
D.社会工程学；伪装的身份；精心策划；前期的准备；一些特征

68.内容安全是我国信息安全保障工作中的一个重要环节，互联网所带来的数字资源大爆发是使得内容安全越来受到重视，以下哪个描述不属于内容安全的范畴( )。
A 某杂志在线网站建立内容正版化审核团队、对向网站投稿的内容进行版权审核，确保无侵犯版权行为后才能在站上进行发布
B.某网站采取了技术措施，限制对同一 IP 地址对网站的并发连接，避免爬虫通过大量的访问采集网站发布数据
C.某论坛根据相关法律要求，进行了大量的关键词过滤，使用户无法发布包含被过滤关键词的相关内容
D.某论坛根据国家相关法律要求，为了保证用户信息泄露，对所有用户信息，包括用户名、密码、身份证号等都进行了加密的存储

69.恶意软件分析是快速准确的识别恶意软件行为，清除恶意软件，保护系统和其他应用程序安全的重要措施。随着恶意软件抗分析技术的发展，恶意软件广泛使用了加壳、加密、混淆等抗分析技术，对恶意软件的分析难度越来越大。对恶意代码分析的研究已经成为信息安全领域的一个研究热点。小赵通过查阅发现一些安全软件的沙箱功能目实际上是虚拟化技术的应用，是动态分析中广泛采用的一种技术。小赵列出了一些动态分析的知识，其中错误的是（　　）。
A 动态分析是指在虚拟运行环境中，使用测试及监控软件，检测恶意代码行为，分析其执行流程及处理数据的状态，从而判断恶意代码的性质，并掌握其行为特点
B.动态分析针对性强，并且具有较高的准确性，但由于其分析过程中覆盖的执行路径有限，分析的完整性难以保证
C.动态分析通过对其二进制文件的分析，获得恶意代码的基本结构和特征，了解其工作方式和机制

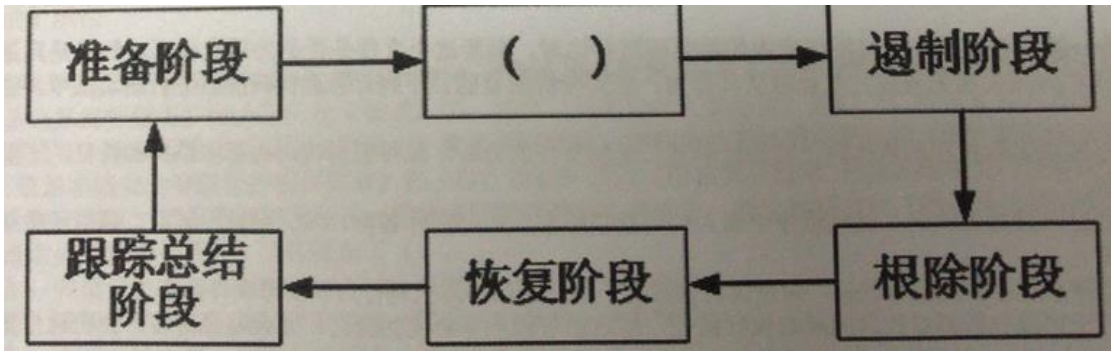
D.动态分析通过监控系统进程、文件和注册表等方面出现的非正常操作和变化，可以对恶意代码非法行为进行分析

70.安全评估技术采用（　　）这一工具，它是一种能够自动检测远程或本地主机和网络安全性弱点的程序。
A.安全扫描器　　B.安全扫描仪　C.自动扫描器　D.自动扫描仪

71.小张在一不知名的网站上下载了鲁大师并进行了安装，电脑安全软件提示该软件有恶意捆绑，小张惊出一身冷汗，因为他知道恶意代码将随之进入系统后会对他的系统信息安全造成极大的威胁，那么恶意代码的软件部署常用的实现方式不包括（　　）
A.攻击者在获得系统的上传权限后，将恶意代码部署到目标系统
B.恶意代码自身就是软件的一部分，随软件部署传播
C 内嵌在软件中，当文件被执行时进入目标系统
D.恶意代码通过网上激活

72.操作系统是作为一个支撑软件，使得你的程序或别的应用系统在上面正常运行的一个环境。操作系统提供了很多的管理功能，主要是管理系统的软件资源和硬件资源。操作系统软件自身的不安全性，系统开发设计的不周而留下的破绽，都给网络安全留下隐患。某公司的网络维护师为实现该公同操作系统的安全目标，按书中所学建立了相应的安全机制，这些机制不包括（　　）
A.标识与鉴别
B.访问控制
C.权限管理
D 网络云盘存取保护

73.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，既包括预防性措也包括事件发生后的应对措施。应急响应方法和过程并不是唯一的，在下面的应急响应管理流程图中，空白方框填写正确的选项是（　　）



A.培训阶段 B.文档阶段 C.报告阶段 D.检测阶段

74.即时通讯安全是移动互联网时代每个用户和组织机构都应该认真考虑的问题，特别对于使用即时通讯进行工作交流和协作的组织机构。安全使用即时通讯应考虑许多措施，　下列描施中错误的是(　　)

A.如果经费许可，可以使用自建服务器的即时通讯系统
B.在组织机构安全管理体系中制定相应安全要求，例如禁止在即时通讯中传输敏感及以上级别的文档；建立管理流程及时将员工移除等
C.选择在设计上已经为商业应用提供安全防护的即时通讯软件，例如提供传输安全性保护等即时通讯
D.涉及重要操作包括转账无需方式确认

75. 如果有一名攻击者在搜索引擎中搜索“. doc+ XXX. com"找到 XXX. com 网站上所有的 word 文档。该攻击者通过搜索".mdb"、 ".ini”+城名，找到该域名下的 mdb 库文件、ini 配置文件等非公开信息，通过这些敏感信息对该网站进行攻击，请问这属于(　　)
A.定点挖掘
B.攻击定位
C.网络实施嗅探
D.溢出攻击

76.以下哪些因素属于信息安全特征?
A.系统和网络的安全
B.系统和动态的安全
C.技术、管理、工程的安全
D.系统的安全； 动态的安全；无边界的安全；非传统的安全

77.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　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

78.某集团公司信息安全管理员根据领导安排制定了下一-年度的培训工作计划，提出了四大培训任务和目标，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岗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，实现全员信息安全意识教育

79.信息应按照其法律要求、价值、对泄露或算改的(　　)和关键性予以分类。信息资产的所有者应对其分类负责。分类的结果表明了(　　)，该价值取快于其对组织的敏够性和关键性如保密性、完整性和有效性。信息要进行标记并体现其分类，标记的规程需要涵盖物理和电子格式的(　　) 。分类信息的标记和安全

处理是信息共享的一个关键要求。(　　)和元数据标签是常见的形式。标记应易于辨认，规程应对标记附着的位置和方式给出指导，并考虑到信息被访问的方式和介质类型的处理方式。组织要建立与信息分类一致的资产处理、 加工、存储和(　　)。
A.敏感性；物理标签；资产的价值；信息资产；交换规程
B.敏感性；信息资产；资产的价值；物理标签；交换规程
C.资产的价值；敏感性；信息资产；物理标签；交换规程
D.敏感性；资产的价值；信息资产；物理标签；交换规程

80.杀毒软件一般是通过对代码与特征库中的特征码进行比对，判断这个文件是否是为恶意代码，如果是则进一步联系到病毒库中对该病毒的描述，从而确认其行为，达到分析的目的。下列对恶意代码静态分析的说法中，错误的是(　　)
A.静态分析不需要实际执行恶意代码，它通过对其二进制文件的分析，获得恶意代码的基本结构和特征，了解其工作方式和机制
B.静态分析通过查找恶意代码二进制程序中嵌入的可疑字符串，如:文件名称、URL 地址、域名、调用函数等，来进行分析判断
C.静态分析检测系统函数的运行状态，数据流转换过程，能判别出恶意代码行为和正常软件操作
D.静态分析方法可以分析恶意代码的所有执行路径，但是随着程序复杂度的提高，冗余路径增多，会出现分析效率很低的情况

81.数据库是一个单位或是一个应用领城的通用数据处理系统，它存储的是属于企业和事业部门、团体和个人的有关数据的集合。数据库中的数据是从全局观点出发建立的，按一定的数据模型进行组织、 描述和存储。其结构基于数据间的自然联系，从而可提供一切必要的存取路径，且数据不再针对某一应用，而是面向全组织，具有整体的结构化特征。数据库作为应用系统数据存储的系统，毫无疑间会成为信息安全的重点防护对象。数据库安全涉及到数据资产的安全存储和安全访问，对数据库安全要求不包括下列(　　)
A.向所有用户提供可靠的信息服务
B 拒绝执行不正确的数据操作
C.拒绝非法用户对数据库的访问
D.能跟踪记录，以便为合规性检查、安全责任审查等提供证据和迹象等

82.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，为信息安全产业发展创造一个良好的竞争环境

83.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/T

20274. 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

84.风险评估相关政策， 目前主要有（ ）。(国信办[2006]5 号)。主要内容包括分析信息系统资产的（ ），评估信息系统面临的（ ）、存在的（ ）、已有的安全措施和残余风险的影响等、两类信息系统的（ ）、涉密信息系统参照“分级保护”、非涉密信息系统参照“等级保护”。
A.《关于开展信息安全风险评估工作的意见》；重要程度；安全威胁；脆弱性；工作开展
B.《关于开展风险评估工作的意见》；安全威胁；重要程度；脆弱性；工作开展
C. 《关于开展风险评估工作的意见》；重要程度；安全威胁；脆弱性；工作开展
D.《关于开展信息安全风险评估工作的意见》；脆弱性；重要程度；安全威胁；工作开展

85.（)在实施攻击之前，需要尽量收集伪装身份（)，这些信息是攻击者伪装成功的（)。例如攻击者要伪装成某个大型集团公司总部的（)，那么他需要了解这个大型集团公司所处行业的一些行规或者（)、公司规则制度、组织架构等信息，甚至包括集团公司中相关人员的绰号等等。
A.攻击者；所需要的信息；系统管理员；基础；内部约定
B.所需要的信息；基础；攻击者；系统管理员；内部约定
C.攻击者；所需要的信息；基础；系统管理员；内都约定
D.所需要的信息；攻击者；基础；系统管理员；内部约定

86.小红和小明在讨论有关于现在世界上的 IP 地址数量有限的问题，小红说他看到有新闻说在 2011 年 2 月 3 日，全球互联网 IP 地址相关管理组织宣布现有的互联网 IP 地址已于当天划分给所有的区城互联网注册管理机构，IP 地址总库已经枯竭，小明吓了一跳觉得以后上网会成问题，小红安慰道，不用担心，现在 IPv6 已经被试用它有好多优点呢，以下小红说的优点中错误的是（)
A.网络地址空间的得到极大扩展
B. IPv6 对多播进行了改进，使得具有更大的多播地址空间
C.繁杂报头格式
D.良好的扩展性

87.方法指导类标准士要包括 GB/T. _25058-2010_《信息安全技术_信息系统安全等级保护实施指南》GB/T25070-2010 《信息系统等级保护安全设计技术要求》等。其中《等级保护实施指南》原以（)政策文件方式发布，后修改后以标准发布。这些标准主要对如何开展（)做了详细规定。状况分析类标准主要包括 GB/T 28448- 2012《信息安全技术信息系统安全等级保护测评要求》和 GB/T

28449-2012《信息安全技术信息系统安全等级保护测评过程指南》等。其中在(　)工作期间还发布过《等级保护测评准则》等文件，后经过修改以《等级保护测评要求》发布。这些标准主要对如何开展(　)工作做出了(　)
A 公安部；等级保护试点；等级保护工作；等级保护测评；详细规定
A.公安部；等级保护工作；等级保护试点；等级保护测评；详细规定
C.公安部；等级保护工作；等级保护测评；等级保护试点；详细规定
D.公安部；等级保护工作；等级保护试点；详细规定；等级保护测评

88.下列选项中，对风险评估文档的描述中正确的是(　)
A.评估结果文档包括描述资产识别和赋值的结果，形成重要资产列表
B.描述评估结果中不可接受的风险制定风险处理计划。选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性的《风险评估程序》
C.在文档分发过程中作废文档可以不用添加标识进行保留
D 对于风险评估过程中形成的相关文档行，还应规定其标识、储存、保护、检索、保存期限以及处置所需的控制

89.下列软件开发模型中，支持需求不明确，特别是大型软件系统的开发，并支持多种软件开发方法的模型是(　　)。
A.原型模型　B.瀑布模型　C.喷泉模型　D.螺旋模型

90.供电安全是所有电子设备都需要考虑的问题，只有持续平稳的电力供应，才能保障电子设备工作稳定可靠。因此电力供应需要解决问题包括两个，一是确保电力供应不中断、二是确保电力供应平稳。下列选项中，对电力供应的保障措施的描述正确的是(　　)。
A.可以采用双路供电来确保电力供应稳定性
B.　UPS 可提供持续、平稳的电力供应，不会受到电涌的影响
C.可以部署电涌保护器来确保电力供应稳定性
D.发动机供电是目前电力防护最主要的技术措施

91.漏洞扫描是信息系统风险评估中的常用技术措施，定期的漏洞扫描有助于组织机构发现系统中存在的安全漏洞。漏洞扫描软件是实施漏洞扫描的工具，用于测试网络、操作系统、数据库及应用软件是否存在漏洞。某公司安全管理组成员小李对漏洞扫描技术和工具进行学习后有如下理解，其中错误的是(　　)
A.主动扫描工作方式类似于 IDS　(Intrusion　Detection　Systems)
B.　CVE　(Comon　Vulnerabilities　&　Exposures)为每个漏洞确定了唯一的名称和标准化的描述 C.　X.　Scanner 采用多线程方式对指定 IP 地址段进行安全漏洞扫描
D.　ISS 的 System　Scanmer　通过依附于主机上的扫描器代理侦测主机内部的漏洞

92.组织应开发和实施使用(　)来保护信息的策略，基于风险评估，宜确定需要的保护级别，并考虑需要的加密算法的类型、强度和质量。当实施组织的(　)时，宜考虑我国应用密码技术的规定和限制，以及(　)跨越国界时的问题。组织

应开发和实施在密钥生命周期中使用和保护密钥的方针。方针应包括密钥在其全部生命周期中的管理要求，包括密钥的生成、存储、归档、检索、分配、卸任和销毁。宜根据最好的实际效果选择加密算法、密钥长度和使用习惯。适合的(　　)要求密钥在生成、存储、归档、检索、分配、卸任和销毁过程中的安全。宜保护所有的密钥免遭修改和丢失。另外，秘密和私有密钥需要防范非授权的泄露。用来生成、存储和归档密钥的设备宜进行(　　)　。
A.加密控制措施；加密信息；密码策略；密钥管理；物理保护
B.加密控制措施；密码策略；密钥管理；加密信息；物理保护
C.加密控制措施；密码策略；加密信息；密钥管理；物理保护
D.加密控制措施；物理保护；密码策略；加密信息；密钥管理

93.由于病毒攻击、非法入侵等原因，校园网整体瘫痪，或者校园网络中心全部DNS、　主 WEB 服务器不能正常工作。由于病毒攻击、非法入侵、人为破坏或不可抗力等原因，造成校园网出口中断，属于以下哪种级别事件(　　)
A.特别重大事件 B.重大事件 C.较大事件 D.一般事件

94.安全审计是事后认定违反安全规则行为的分析技术，在检测违反安全规则方面、准确发现系统发生的事件以对事件发生的事后分析方面，都发挥着巨大的作用。但安全审计也有无法实现的功能，以下哪个需求是网络安全审计无法实现的功能(　　)
A.发现系统中存储的漏洞和缺陷
B.发现用户的非法操作行为
C.发现系统中存在后门及恶意代码
D.发现系统中感染的恶意代码类型及名称

95.　数位物件识别号(Digital　Object　Identifier,　简称 DOI)是一套识别数位资源的机制，涵括的对象有视频报告或书籍等等。它既有一套为资源命名的机制，也有一套将识别号解析为具体位址的协定。　DOI　码由前缀和后缀两部分组成，之间用″/”分开，并且前缀以“　.　”再分为两部分。以下是一个典型的 DOI 识别号 10.　1006/jmbi.　1998.　2354，下列选项错误的是(　　)
A.　“10.1006”是前缀，由国际数位物件识别号基金会确定
B.　“10”为 DOI 月前唯一的特定代码，用以将 DOI 与其他采用同样技术的系统区分开
C.　“1006”是注册代理机构的代码，或出版社代码，用于区分不同的注册机构
D.　后缀部分为:　jmbi.　1998　.2354,　由资源发行者自行指定，用于区分一个单独的数字资料，不具有唯一性

96.某网盘被发现泄露了大量私人信息，通过第三方网盘搜索引擎可查询到该网盘用户的大量照片、通讯录。网盘建议用户使用“加密分享”功能，以避免消息泄露，“加密分享”　可以采用以下哪些算法(　　)
A.　MD5 算法，SHA-1　算法
B.　DSA 算法，RSA 算法
C.SHA-1 算法，SM2 算法
D.RSA 算法，SM2　算法

97.作为单位新上任的 CSO，你组织了一次本单位的安全评估工作以了解单位安全现状。在漏洞扫描报　现了某部署在内网且仅对内部服务的业务系统存在一个漏洞，对比上一年度的漏洞扫描报告，发现这个 经报告出来，经询问安全管理员得知，这个业务系统开发商已经倒闭，因此无法修复。对于这个问题，　处理(　)
A.向公司管理层提出此问题，要求立即立项重新开发此业务系统，避免单位中存在这样的安全风险
B.既然此问题不是新发现的问题，之前已经存在，因此与自己无关，可以不予理会
C.让安全管理人员重新评估此漏洞存在的安全风险并给出进一步的防护措施后再考虑如何处理
D.让安全管理员找出验收材料看看有没有该业务系统源代码，自己修改解决这个漏洞

98.以下哪项网络攻击会对《网络安全法》定义的网络运行安全造成影响?
A. DDos 攻击
B.网页篡改
C.个人信息泄露
D.发布谣言信息

99.软件工程方法提出起源于软件危机，而其目的应该是最终解决软件的问题的是(　)。
A.质量保证
B.生产危机
C.生产工程化
D.开发效率

100.风险评估的过程包括(　)、(　)、(　)和(　)四个阶段。在信息安全风险管理过程中，风险评估　建立阶段的输出，形成本阶段的最终输出《风险评估报告》，此文档为风险处理活动提供输入。(　)风险评估的四个阶段。
A.风险评估准备；风险要素识别；风险分析；监控审查；风险结果判定；沟通咨询
B.风险评估准备；风险要素识别；监控审查；风险分析；风险结果判定；沟通咨询
C.风险评估准备；监控审查；风险要素识别；风险分析；风险结果判定；沟通咨询
D.风险评估准备；风险要素识别；风险分析；风险结果判定；监控审查；沟通咨询

参考答案

题号	1	2	3	4	5	6	7	8	9	10
答案	C	A	A	D	D	A	C	B	B	A
题号	11	12	13	14	15	16	17	18	19	20
答案	D	B	B	B	D	C	C	D	C	B
题号	21	22	23	24	25	26	27	28	29	30
答案	D	C	D	A	B	A	A	C	B	A
题号	31	32	33	34	35	36	37	38	39	40
答案	C	B	B	B	D	A	B	B	D	C
题号	41	42	43	44	45	46	47	48	49	50
答案	C	B	A	A	A	D	D	C	B	A
题号	51	52	53	54	55	56	57	58	59	60
答案	B	B	A	C	A	D	A	A	A	C
题号	61	62	63	64	65	66	67	68	69	70
答案	C	B	B	A	D	B	A	D	C	A
题号	71	72	73	74	75	76	77	78	79	80
答案	D	D	D	D	A	D	C	D	D	C
题号	81	82	83	84	85	86	87	88	89	90
答案	A	D	D	A	C	C	B	B	D	C
题号	91	92	93	94	95	96	97	98	99	100
答案	A	C	C	A	D	D	C	A	C	D