1.在某信息系统采用的访问控制策略中，如果可以选择值得信任的人担任 各级领导对客体实施控制，且各级领导可以同时修改它的访问控制表，那 么该系统的访问控制模型采用的自主访问控制机制的访问许可模式是（）。

A.自由型　　B.有主型　　C.树状型　　D.等级型

答案：D

3.以下关于开展软件安全开发必要性描错误的是？（）

A．软件应用越来越广泛

B.软件应用场景越来越不安全

C．软件安全问题普遍存在

D.以上都不是

答案：D

4.软件危机是指落后的软件生产方式无法满足迅速增长的计算机软件需 求，从而导致软件开发与维护过程中出现一系列严重问题的现象。为了克 服软件危机，人们提出了用（）的原理来设计软件，这就是软件工程诞生 的基础

A．数学　　B.软件学　　C.运筹学　　D.工程学

答案：D

6.在设计信息系统安全保障方案时，以下哪个做法是错误的

A．要充分企切合信息安全需求并且实际可行

B．要充分考虑成本效益，在满足合规性要求和风险处置要求的前提下，尽量 控制成本

C．要充分采取新技术，在使用过程中不断完善成熟，精益求精，实现技术投 入保障要求

D．要充分考虑用户管理和文化的可接受性，减少系统方案实验障碍

答案：C

7.灾备指标是指信息安全系统的容灾抗毁能力，主要包括四个具体指标：恢 复时间目标（Recovery Time Oh jective,RTO）.恢复点目标（Recovery Point Objective,RPO）降级操作目标（Degraded Operations Ob jective-DOO）和网络恢复目标（NeLwork Recovery Ob jective-NRO）,小华准备为其工作的 信息系统拟定恢复点目标 RPO=0，以下描述中，正确的是（）。

A．RPO=0，相当于没有任何数据丢失，但需要进行业务恢复处理，覆盖原有 信息

B. RPO=0，相当于所有数据全部丢失，需要进行业务恢复处理。修复数据丢 失

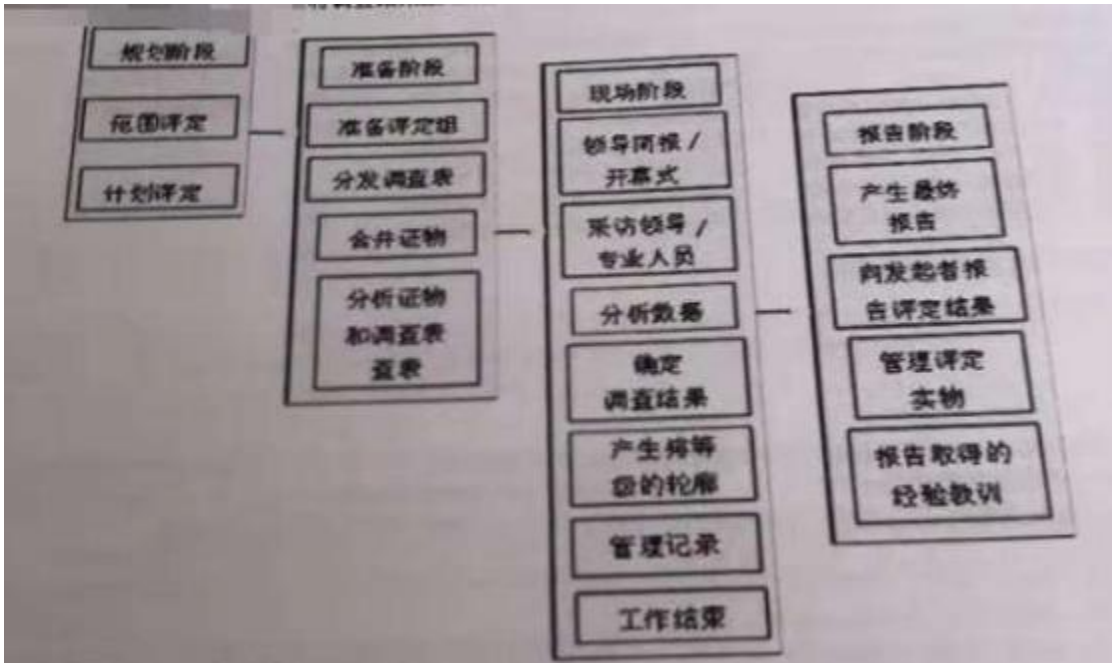
C．RPO=0，相当于部分数据丢失，需要进行业务恢复处理，修复数据丢失

D．RPO=0，相当于没有任何数据丢失，且不需要进行业务恢复处理

答案：D

8.下图显示了 SSAM 的四个阶段和每个阶段工作内容。与之对应，() 的目的 是

建立评估框架，并为现场阶段准备后勤方面的工作。()的目的是准备评估 团队进行现场活动，并通过问卷进行数据的初步收集和分析。()主要是探索 初步数据分析结果，以及为被评组织的专业人员提供与数据采集和证实过程 的机会，小组对在此就三个阶段中采集到的所有数据进行 ()。并将调查结果 呈送个发起者



A．现场阶段；规划阶段；准备阶段；最终分析

B.准备阶段；规划阶段；现场阶段；最终分析

C．规划阶段；现场阶段；准备阶段；最终分析

D．规划阶段；准备阶段；现场阶段；最终分析

答案：D

9.组织应依照已确定的访问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问。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和程 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）的访问宜严格控制，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， 可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

答案：A

10.信息时流动的，在信息的流动过程中必须能够识别所有可能途径的()与 ()；面对于信息本身，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，不同的截体下，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；截体；环境；永久性；风险管理

B．基础；依据；截体；环境；风险管理；永久性

C．截体；环境；风险管理；永久性；基础；依据

D．截体；环境；基础；依据；风险管理；永久性

答案：D

11.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，提出了四个培训任务和目标。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位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（网路管理员、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

答案：A

13.某项目组进行风险评估时由于时间有限，决定采用基于知识的分析方法， 使用基于知识的分析方法进行风险评估，最重要的在于评估信息的采集，该项目组对信息源进行了讨论，以下说法中不可行的是（）

A．可以通过对当前的信息安全策略和相关文档进行复查采集评估信息

B. 可以通过进行实施考察的方式采集评估信息

C．可以通过建立模型的方法采集评估信息

D．可以制作问卷，进行调查

答案：C

14.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终随之进入系 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见 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．内镶在软件中，当文件被执行时进入目标系统

D．恶意代码通过网上激活

答案：D

15.（）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；内部约定

D．所需要的信息；攻击者；基础；系统管理员；内部约定

答案：A

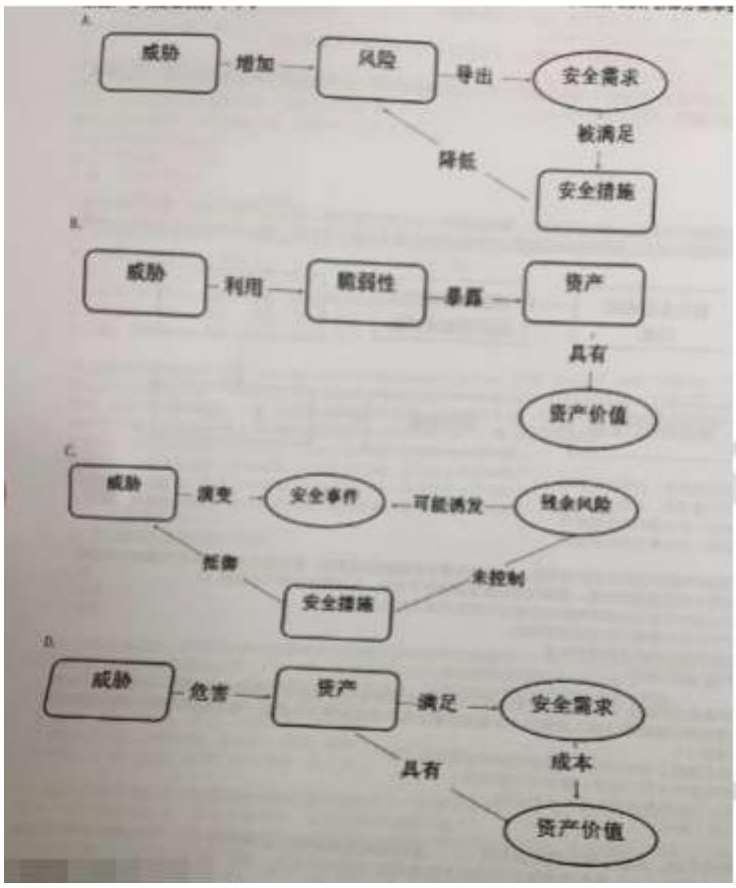
16.1993 年至 1996 年，欧美六国和美国商务部国家标准与技术局共同制定了一个供欧美各国通用的信息安全评估标准，简称 CC 标准，该安全评估标准的全称为（）

A.《可信计算机系统评估准则》　　B.《信息技术安全评估准则》

C .《可信计算机产品评估准则》　　D.《信息技术安全通用评估准则》

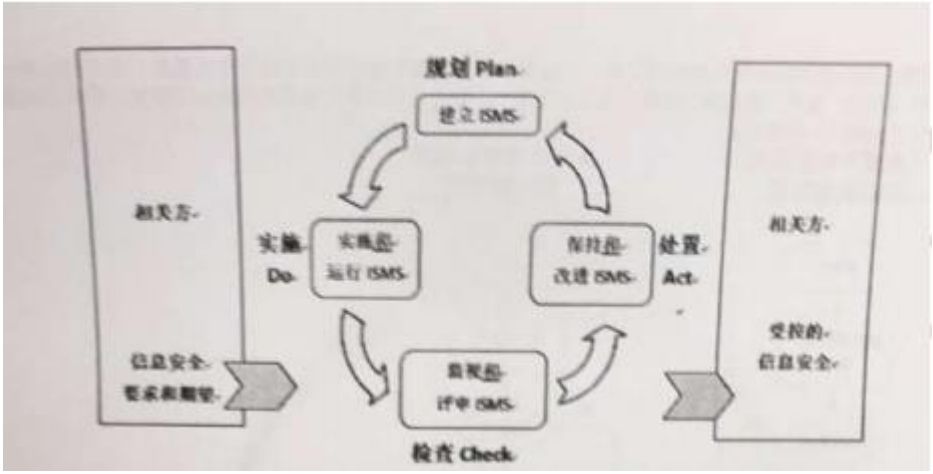
答案：D

17.风险评估的基本要素包括脆弱性、资产、威胁、风险及安全措施，下面给 出的风险评估部分基本要素之间的关系图，哪项是错误的（ ）。



答案：D

18.下图描绘了信息安全管理体系的 PDCA 模型其中，建立 ISMS 中，组织应根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界， 包括对范围任何删减的详细说明和正当性理由。组织应根据业务、组织、位 置、资产和技术等方面的特性，监视和评审 ISMS（）。实施和运行 ISMS 中， 组织应为管理信息安全风险识别适当的（）、资源、职责和优选顺序，监视和 评审 ISMS 中，组织应执行监视与评审规程和其他（）。以迅速检测过程运行 结果中的错误，迅速识别图的和得逞的安全违规和事件，使管理者能够确定 分配给人员的安全活动或通过信息技术实施的安全活动是否按期望执行，通 过使用指示器帮助检测安全事态并预防安全事件，确定解决安全违规的措施 是否有效，保持和改进 ISMS 中，组织应经常进行 ISMS 改进，采取合适的纠 正和（），从其他组织和组织自身的安全经验中（）。



A.方针； 管理措施； 控制措施； 预防措施； 吸取措施

B．方针； 控制措施； 管理措施； 预防措施； 吸取措施

C．方针； 预防措施； 管理措施； 控制措施； 吸取措施

D．方针； 吸取措施； 管理措施； 控制措施； 预防措施

答案： A

19.计算机漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺 陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。在病毒肆意 的信息不安全时代，某公司为减少计算机系统漏洞，对公司计算机系统进行 了如下措施，其中错误的是（）

A．减少系统日志的系统开销

B．禁用或删除不需要的服务，降低服务运行权限

C．设置策略避免系统出现弱口令并对口令猜测进行防护

D .对系统连续进行限制，通过软件防火墙等技术实现对系统的端口连续进行 控制

答案：A

20.某 IT 公司针对信息安全事件已建立了完善的预案，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 CSO，请你指出存在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 事件分类分级分级指南》，分为 7 个基本类别，预案符合国家相关标准

答案：A

21.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

答案：B

22.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

答案：D

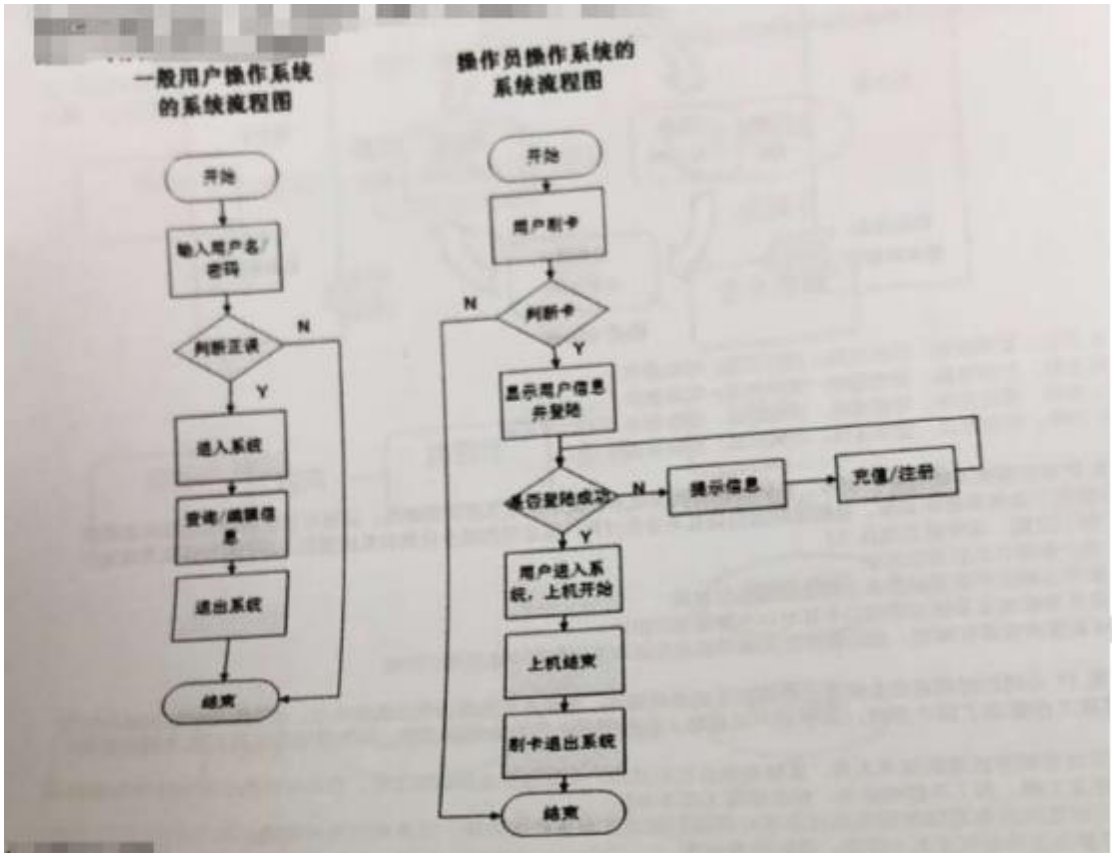
23.访问控制方法可分为自主访问控制、强制访问控制和基于角色访问控制， 它们具有不同的特点和应用场景。如果需要选择一个访问控制模型，要求能 够支持最小特权原则和职责分离原则，而且在不同的系统配置下可以具有不 同的安全控制，那么在（1）自主访问控制，（2）强制访问控制，（3）基于角 色的访问控制（4）基于规则的访问控制中，能够满足以上要求的选项有（）

A.只有（1）（2）　　B.只有（2）（3）

C.只有（3）（4）　　D.只有（4）

答案：C

24.系统流程图是描绘系统物理模型的传统工具。(如下图）它的基本思想是 用图形符号以黑盒子形式描绘系统里面的每个部件（程序、文件、数据库、 表格、人工过程等)。表达信息在各个部件之间流动的情况，那么系统流程图 用于可行性分析的（）的描述。



A．当前运行系统　　B.当前逻辑模型

C．目标系统　　D.新系统

答案：B

25.国家对信息安全建设非常重视，如国家信息化领导小组在（）中确定要求，“信息安全建设是信息化的有机组成部分，必须与信息化同步规划、同步建 设。

各地区各部门在信息化建设中，要同步考虑信息安全建设，保证信息安 全设施的运行维护费用。”国家发展改革委所下发的（）要求；电子政务工程 建设项目必须同步考虑安全问题，提供安全专项资金，信息安全风险评估结 论是项目验收的重要依据。在我国 2017 年正式发布的（）中规定“建设关键 信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全 技术措施同步规划、同步建设、同步使用。”信息安全工程就是要解决信息系 统生命周期的“过程安全”问题。

A .《关于加强信息安全保障工作的意见》;《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》;《网络安全法》

B《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》;《关 于加强信息安全保障工作的意见》;《网络安全法》

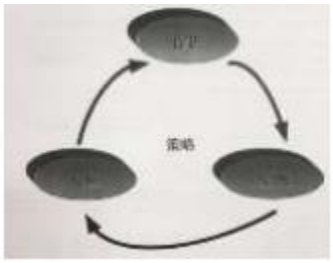
C .《网络安全法》;《关于加强信息安全保障工作的意见》;《关于加强国家电 子政务工程建设项目信息安全风险评估工作的通知》

D .《网络安全法》;《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》;《关于加强信息安全保障工作的意见》

答案：A

26 在 PDR 模型的基础上，发展成为了 （Policy-Protection-Detection-Response,PPDR）模型，即策略-保护-检测 -响应。模型的核心是：所有的防护、检测、响应都是依据安全策略实施的。 如图所示。在 PPDR 模型中，策略指的是信息系统的安全策略，包括访问控制 策略、加密通信策略、身份认证测录、备份恢复策略等。策略体系的建立包 括安全策略的制定、（）等；防护指的是通

过部署和采用安全技术来提高网络 的防护能力，如（）、防火墙、入侵检测、加密技术、身份认证等技术；检测 指的是利用信息安全检测工具，监视、分析、审计网络活动，了解判断网络 系统的（）。检测这一环节，使安全防护从被动防护演进到主动防御，是整个 模型动态性的体现，主要方法包括；实时监控、检测、报警等；响应指的是 在检测到安全漏洞和安全事件，通过及时的响应措施将网络系统的（）调整 到风险最低的状态，包括恢复系统功能和数据，启动备份系统等。启动备份 系统等。其主要方法包括：关闭服务、跟踪、反击、消除影响等。



A．评估与执行；访问控制；安全状态；安全性

B．评估与执行；安全状态；访问控制；安全性

C．访问控制；评估与执行；安全状态；安全性

D．安全状态，评估与执行；访问控制；安全性

答案：A

27.现如今的时代是信息的时代，每天都会有大量的信息流通或交互，但自从 斯诺登曝光美国政府的“棱镜”计划之后，信息安全问题也成为了每个人乃 至整个国家所不得不重视的问题，而网络信息对抗技术与电子信息对抗技术 也成为了这个问题的核心。某公司为有效对抗信息收集和分析，让该公司一 位网络工程师提出可行的参考建议，在该网络工程师的建议中错误的是（）

A.通过信息安全培训，使相关信息发布人员了解信息收集的风险

B.发布信息应采取最小原则，所有不是必要的信息都不发布

C．重点单位应建立信息发布审查机制，对发布的信息进行审核，避免敏感信 息的泄露

D．增加系统中对外服务的端口数量，提高会话效率

答案：D

28.分析针对 Web 的攻击前，先要明白 http 协议本身是不存在安全性的问题的，就是说攻击者不会把它当作攻击的对象。而是应用了 http 协议的服务器 或则客户端、以及运行的服务器的 wed 应用资源才是攻击的目标。针对 Web 应用的攻击，我们归纳出了 12 种，小陈列举了其中的 4 种，在这四种当中错 误的是（）

A.拒绝服务攻击　　B.网址重定向　　C.传输保护不足　　D.错误的访问控制

答案：D

29.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体统突发事件能力，较少突发事件造成的 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

答案：C

30.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，阶段较多，而其中最重要的是软件的编码阶 段做好安全措施，就可以解决 90%以上的安全问题

B．应当今早在软件开发的需求和设计阶段就增加一定的安全措施，这样可以 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，微软提出的完全开发生命周期的最大特点是 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，充分的安全测试可以避免安全问题的产生

答案：B

31.在新的信息系统或增强已有()业务要求陈述中，应规定对安全控制措施的 要求。信息安全的系统要求与实施安全的过程宜在信息系统项目的早期阶段 被集成，在早期如设计阶段引入控制措施的更高效和节省。如果购买产品， 则宜遵循一个正式的（）过程。通过（）访问的应用易受到许多网络威胁， 如欺诈活动、合同争端和信息的泄露或修改。因此要进行详细的风险评估并 进行适当的控制，包括验证和保护数据传输的加密方法等，保护在公共网络 上的应用服务以防止欺诈行为、合同纠纷以及未经授权的（）。应保护涉及到 应用服务交换的

信息以防不完整的传输、路由错误、未经授权的改变、擅自 披露、未经授权的（）。

A．披露和修改；信息系统；测试和获取；公共网路；复制或重播

B.信息系统；测试和获取；披露和修改；公共网路；复制或重播

C．信息系统；测试和获取；公共网路；披露和修改；复制或重播

D．信息系统；公共网路；测试和获取；披露和修改；复制或重播

答案：C

32.某贸易公司的 OA 系统由于存在系统漏洞，被攻击者上传了木马病毒并删除了系统中的数据，由于系统备份是每周六进行一次，事件发生时间为周三， 因此导致该公司三个工作日的数据丢失并使得 OA 系统在随后两天内无法访 问，影响到了与公司有业务往来部分公司业务。在事故处理报告中，根据 GB/Z20968-2007《信息安全事件分级分类指南》，该事件的准确分类和定级应 该是（）

A．有害程序事件 特别重大事件（I 级）

B．信息破坏事件 重大事件（II 级）

C．有害程序事件 较大事件（III 级）

D．信息破坏事件 一般事件(IV 级)

答案：D

33.SSAM 过程的主要工作产品是（）和（）。（）包括（）和（）．（）表示组 织的每个 PA 的能力水平。（）考察了评估组织的优缺点。它通常是为被评估 方开

发的，但可以被评估方的要求提交给评估组织。评估报告仅供被评估方 使用，并包括每个调查结果及其对被评估方需求影响的详细信息。

A．评估报告；调查结果简报；调查结果简报；评估资料；评估结果清单；评 级概况调查结果

B.调查结果简报；评估报告；调查结果简报；评估资料；评估结果清单；评 级概况； 调查结果

C．调查结果简报；评估报告；评估资料；调查结果简报；评级概况；调查结 果

D．调查结果简报；评估报告；调查结果简报；评级概况；评估资料；评估结 果清单；调查结果

答案：B

34.2016 年 12 月 27 日，经中央网路安全和信息化领导小组批准，国家互联 网信息办公室发布《国家网络空间安全战略》（以下简称：“战略”）。全文共 计（）部分，6000 余字。其中主要对我国当前面临的网络空间安全 7 大机遇 思想，阐明了中国关于网络空间发展和安全的重大立场和主张，明确了战略 方针和主要任务，切实维护国家在网络空间的主权、安全、发展利益，是指 导国家网络安全工作的纲领性文件。《战略》指出，网络空间机遇和挑战并存， 机遇大于挑战。必须坚持积极利用、科学发展、依法管理、确保安全，坚决 维护网络安全，最大限度利用网络空间发展潜力，更好惠及 13 亿多中国人民， 造福全人类，（）。《战略》要求，要以（），贯彻落实创新、协调、绿色、开 放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局， 统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、 开放、合作、有序，

维护国家主权、安全、发展利益，实现建设网络强国的 ()。

A．4 个；总体目标；坚定维护世界和平；总体国家安全观为指导；战略目标

B．5 个；基本目标；坚定维护世界和平；总体国家安全观为指导；战略目标

C．6 个；总体目标；坚定维护世界和平；总体国家安全观为指导；战略目标

D．7 个；基本目标；坚定维护世界和平；总体国家安全观为指导；战略目标

答案：B

35.哪种攻击是攻击者通过各种手段来小号网络宽带或者服务器系统资源，最 终导致被攻击服务器资源耗尽或者系统崩溃而无法提供正常的网络服务 ()

A.拒绝服务 B.缓冲区溢出 C.DNS 欺骗 D.IP 欺骗

答案：A

36.以下关于 VPN 说法正确的是 90

A.VPN 指的是用户自己租用线路，和公共网络物理上完全隔离的、安全的线 路

B.VPN 不能做到信息认证和身份认证

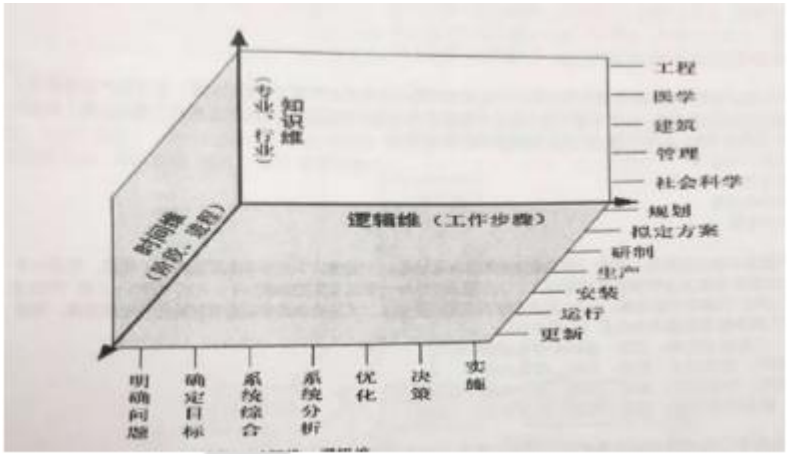
C.VPN 指的是用户通过公用网络建立的临时的、安全的连接

D．VPN 只能提供身份不能提供加密数据的功能

答案：C

37.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

答案：B

38.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

答案：A

39.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

答案：D

40.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

答案：C

41.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

答案：D

42.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

答案：D

43.1998 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

答案：A

44.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

答案：C

45.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

答案：A

46.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；思维；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

答案：C

47.风险评估的工具中，（）是根据脆弱性扫描工具扫描的结果进行模拟攻击 测试，判断被非法访问者利用的可能性，这类工具通常包括黑客工具、脚本 文件。

A．脆弱性扫描工具　　B.渗透测试工具

C. 拓扑发现工具　　D.安全审计工具

答案：B

49.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

答案：B

51.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

答案：D

52.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

答案：B

53.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

答案：A

54.2006 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

答案：B

55.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 不认为新建立的用户 zhang 与原来的用户 zhang 是同一个用户，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

答案：A

56.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

答案：C

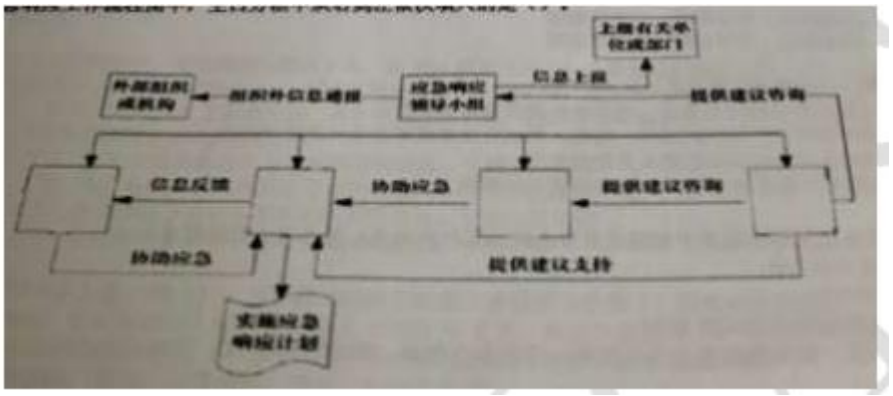
57. 终端访问控制器访问控制系统（Terminal Access Controller Access-Control System,TACACS）由 RFC1492 定义，标准的 TACACS 协议只认证用户是否可以登录系统，目前已经很少使用，TACACS+协议由 Cisco 公司提出，主要应用于 Ciso 公司的产品中，运行与 TCP 协议之上。TACACS+协议分为（）两个不同的过程

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

答案：A

58.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

答案：A

59.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，对它们之间的 关系描述错误的是（）。

A．RBACO 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

答案：C

60.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

答案：B

61.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

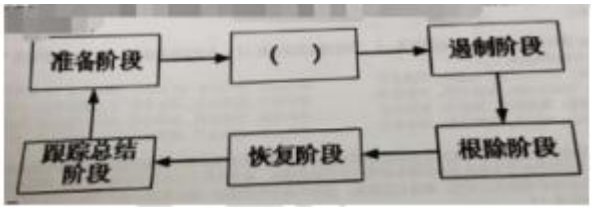
答案：C

62.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

答案：C

63.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（）



A． 培训阶段　　B.文档阶段　　C.报告阶段　　D.检测阶段

答案：D

64.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

答案：A

66.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

答案：D

67.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

答案：D

68.信息安全管理体系 ISMS 是建立和维持信息安全管理体系的（），标准要求组织通过确定信息安全管理系统范围、制定（）、明确定管理职责、以风险评估为基础选择控制目标与控制方式等活动建立信息安全管理体系；体系一旦 建立组织应按体系规定的要求进行运作，保持体系运作的有效性；信息安全 管理体系应形成一定的（），即组织应建立并保持一个文件化的信息安全（）， 其中应阐述被保护的资产、组织安全管理体系应形成一定的（），即组织应建 立并保持一个文件化的信息安全（），其中应阐述被保护的资产、组织风险管 理的方法、控制目标及控制方式和需要的（）.

A.信息安全方针；标准；文件；管理体系；保证程度

B.标准；文件；信息安全方针；管理体系；保证程度

C．标准；信息安全方针；文件；管理体系；保证程度

D．标准；管理体系；信息安全方针；文件；保证程度

答案：C

69.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

答案：C

70.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

答案：A

71.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

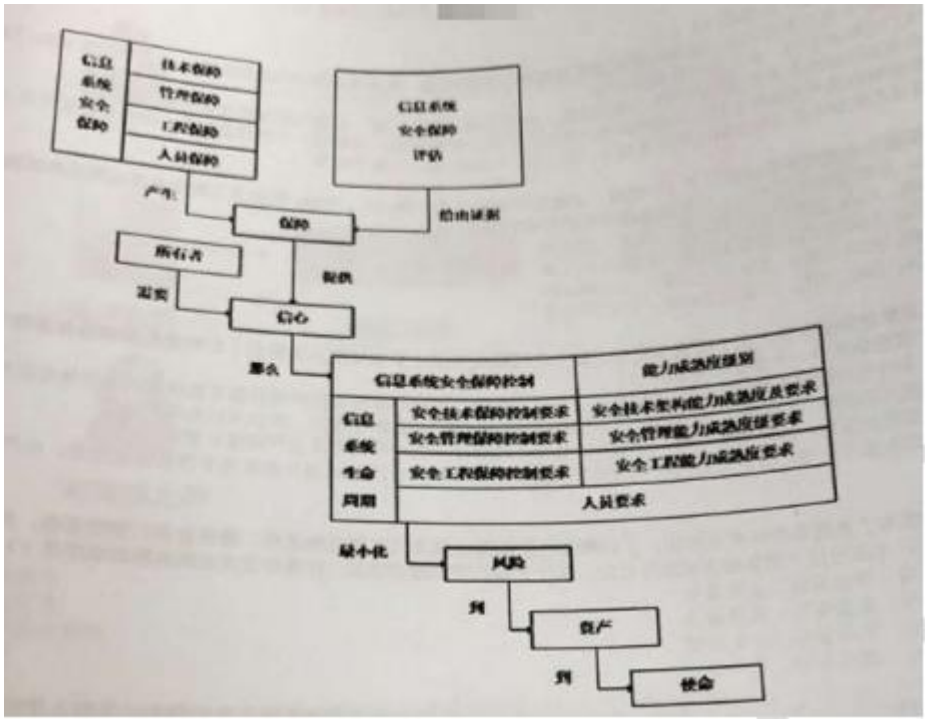
B.内部审计人员质疑是错的，漏洞扫描软件是正版采购，因此扫描结果是准 确的

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

答案：A

72.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

答案：B

74.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

答案：A

75.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，如果对 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

答案：C

76．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.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

答案：C

77.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

答案：B

78.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

答案：C

79.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

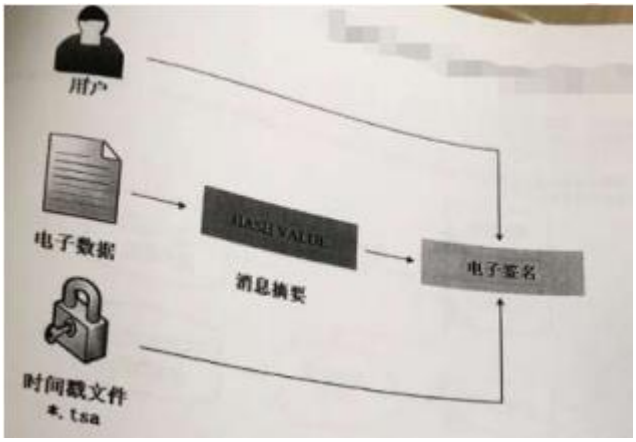
B．完全备份、差量备份、增量备份

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

答案：B

80．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

答案：D

81.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》

答案：A

82.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

答案：B

83.保护-检测-响应（Protection-Detection-Response,PDR）模型是 () 工 作中常用的模型，七思想是承认 () 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

答案：C

86.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

答案：C

87.《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 明确了我国信息安全保障工作的（）加强信息安全保障工作的() 需要重点加强的信息安全保障工作。27 号文的重大意义是。它标志着我国信 息安全保障工作有了（）我国最近十余年的信息安全保障工作都是围绕此政 策性文件来( )的、促进了我国 （）的各项工作。

A.方针: 主要原则: 总体纲领: 展开和推进: 信息安全保障建设

B. 总体要求: 总体纲领: 主要原则: 展开: 信息安全保障建设

C.方针和总体要求: 主要原则: 总体纲领: 展开和推进: 信息安全保障建设

D.总体要求: 主要原则: 总体纲领: 展开: 信息安全保障建设

答案：B

88. 某银行网上交易系统开发项目在最好阶段分析系统运行过程中可能存在 的攻击，请问以下中，哪一项不能降低该系统的受攻击面（）

A. 远程用户或频繁运行身份认证

B. 远程用户访问需要管理员权限

C．关闭不必要的系统服务

D. 当用户访问其账户采用严格的身份认证规则

答案：B

89.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。一种有效的对策是在敌手和它的目标之间配备多种().每种机制都应包括()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: 外边和内部

答案：B

92.关于(网络安全法)域外适用效力的理解，以下哪项是错误的()

A 当前对于境外的网络攻击，我国只能通过向来源国采取抗议

B 对于来自境外的网络安全威胁我国可以组织技术力量进行监测、防御和处 置

C. 对于来自境外的违法信息 我国可以加以阻断传播

D．对于来自境外网络攻击 我国可以追究法律责任

答案：D

93.随机进程名称是恶意代码速迷惑管理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进程名称不固定，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自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代码数字名称

答案：D