### 信息安全管理练习题-2014

**判断题：**

1. 信息安全保障阶段中，安全策略是核心，对事先保护、事发检测和响应、事后恢复起到了统一指导作用。（×）

注释：在统一安全策略的指导下，安全事件的事先预防（保护），事发处理（检测Detection和响应Reaction)、事后恢复（恢复Restoration）四个主要环节相互配合，构成一个完整的保障体系，在这里安全策略只是指导作用，而非核心。

2. 一旦发现计算机违法犯罪案件，信息系统所有者应当在2天内迅速向当地公安机关报案，并配合公安机关的取证和调查。　（×）

注释：应在24小时内报案

3. 我国刑法中有关计算机犯罪的规定，定义了3种新的犯罪类型　（×）

注释：共3种计算机犯罪，但只有2种新的犯罪类型。

( x  )1．客户资料不属于组织的信息资产。

( x  )2．组织的安全要求全部来源于风险评估。

( √ )3．通过使用资源和管理，将输入转化为输出的任意活动，称为过程。

( √ )4．组织必须首先从ISO／IEC27001附录A的控制措施列表中选取控制措施。

( √  )5．风险分析和风险评价的整个过程称为风险评估。

( √  )6．控制措施可以降低安全事件发生的可能性，但不能降低安全事件的潜在影响。

(  x )7．“资产责任人”，要求与信息处理设施有关的所有资产都应由指定人员承担责任。

( x  )8．网站信息由于属于公共可用信息，因此无须实施安全保密措施。

( x  )9．审核范围必须与受审核方信息安全管理体系范围一致。

( √  )10．当组织信息安全管理体系的基础发生重大变化而增加的一次审核称为监督审核。

4. 虽然在安全评估过程中采取定量评估能获得准确的分析结果，但是由于参数确定较为困难，往往实际评估多采取定性评估，或者定性和定量评估相结合的方法。 ( )

5. 信息设备到期报废、淘汰处置或改为他用时，应当清除存储在设备中的信息。（ ）

6. “资产责任人”是指有权限变更资产安全属性的人。( )

7. 所有员工应该发现并报告安全方面的漏洞或弱点以及安全事件。（ ）

8. 系统备份与普通数据备份的不同在于，它备份系统程序、应用程序、参数配置以及数据，以便迅速恢复系统运行。（ ）

9．保护关键业务过程免受信息系统失误或灾难的影响，应定义恢复的优先顺序和时间指标。（ ）

10. 《网络安全法》是2017年1月1日起正式施行。（ ）

**单选题：**

1. 信息安全经历了三个发展阶段，以下( B  )不属于这三个发展阶段。

A. 通信保密阶段　B. 加密机阶段　C. 信息安全阶段　D. 安全保障阶段

2. 信息安全阶段将研究领域扩展到三个基本属性，下列（　C　）不属于这三个基本属性。

A. 保密性　B. 完整性　　C. 不可否认性　　D. 可用性

3. 下面所列的（　A　）安全机制不属于信息安全保障体系中的事先保护环节。

A. 杀毒软件　　B. 数字证书认证　　C. 防火墙　　D. 数据库加密

5. 信息安全领域内最关键和最薄弱的环节是（　D　）。

A. 技术　　B. 策略　　C. 管理制度　　D. 人

6. 信息安全管理领域权威的标准是（　B　）。

A. ISO 15408  B. ISO 17799/ISO 27001(英）  C. ISO 9001  D. ISO 14001

7. 《计算机信息系统安全保护条例》是由中华人民共和国（ A  )第147号发布的。

A. 国务院令　B. 全国人民代表大会令　 C. 公安部令　　D. 国家安全部令

9. 在完成了大部分策略的编制工作后，需要对其进行总结和提炼，产生的结果文档被称为（　A　)。

A. 可接受使用策略AUP　 B. 安全方针　　C. 适用性声明　　D. 操作规范

10. 互联网服务提供者和联网使用单位落实的记录留存技术措施，应当具有至少保存（　C　）天记录备份的功能。

A. 10  B. 30  C. 60  D.90

11. 下列不属于防火墙核心技术的是（　D　）

A. （静态/动态)包过滤技术　　B. NAT技术　　　C. 应用代理技术    D. 日志审计

12. 应用代理防火墙的主要优点是（　B  )

A. 加密强度更高　　B. 安全控制更细化、更灵活　　C. 安全服务的透明性更好　　D. 服务对象更广泛

13. 对于远程访问型VPN来说，（　A　）产品经常与防火墙及NAT机制存在兼容性问题，导致安全隧道建立失败。

A. IPSec VPN  B. SSL VPN  C. MPLS VPN   D. L2TP VPN

注：IPSec协议是一个应用广泛，开放的VPN安全协议，目前已经成为最流行的VPN解决方案。在IPSec框架当中还有一个必不可少的要素: Internet安全关联和密钥管理协议——IKE(或者叫ISAKMP/Oakley)，它提供自动建立安全关联和管理密钥的功能。

14. 1999年，我国发布的第一个信息安全等级保护的国家标准GB 17859-1999，提出将信息系统的安全等级划分为（　D　）个等级，并提出每个级别的安全功能要求。

A. 7   B. 8   C. 6   D. 5

注：该标准参考了美国的TCSEC标准，分自主保护级、指导保护级、监督保护级、强制保护级、专控保护级。

16. 最终提交给普通终端用户，并且要求其签署和遵守的安全策略是（　C　）。

A. 口令策略   B. 保密协议　   C. 可接受使用策略AUP   D. 责任追究制度

 一、选择题(每题1分，共10分)

 (  )1．信息安全中的可用性是指\_\_\_\_\_\_\_C

a)信息不能被未授权的个人，实体或者过程利用或知悉的特性

 b)保护资产的准确和完整的特性

 c)根据授权实体的要求可访问和利用的特性

 d)以上都不对

 (  )2．审核证据是指\_\_\_\_\_\_\_\_B

a)与审核准则有关的，能够证实的记录、事实陈述或其他信息

 b)在审核过程中收集到的所有记录、事实陈述或其他信息

 c)一组方针、程序或要求

 d)以上都不对

 (  )3．\_\_\_\_\_\_ D   属于系统威胁。

 a)不稳定的电力供应

  b)硬件维护失误

  c)软件缺乏审计记录

 d)口令管理机制薄弱

 (  )4．管理体系是指\_\_\_\_\_\_C

a)建立方针和目标并实现这些目标的体系

b)相互关联和相互作用的一组要素

c)指挥和控制组织的协调的活动

 d)以上都不对

 (  )5．信息安全管理实用规则ISO／IECl7799属于\_\_B\_\_\_标准?

a)词汇类标准

 b)要求类标准

 c)指南类标准

 d)以上都不对

 (  )6．在信息安全管理体系\_\_C\_\_阶段应测量控制措施的有效性?

 a)建立

 b)实施和运行

 c)监视和评审

 d)保持和改进

 (  )7．风险评价是指\_\_\_B\_\_\_

 a)系统地使用信息来识别风险来源和估计风险

b)将估计的风险与给定的风险准则加以比较以确定风险严重性的过程

c)指导和控制一个组织相关风险的协调活动

d)以上都不对

(  )8．可使用\_\_\_A\_\_\_\_来保护电子消息的保密性和完整性

a)密码技术

b)通信技术

c)控制技术

d)自动化技术

(  )9．现状不符合文件是指\_\_\_C\_\_\_

a)标准要求的没有写到

b)写到的没有做到

c)做到的没有达到目标

d)以上都不对

(  )10．以下属于计算机病毒感染事件的纠正措施的是\_\_\_\_B\_\_\_\_\_

a)对计算机病毒事件进行响应和处理

b)将感染病毒的计算机从网络中隔离

c)对相关责任人进行处罚

d)以上都不是

 一、选择题

1.以下哪个是信息安全管理标准？ D

A. ISO15408

B. ISO14000

C. ISO9000

D. ISO27001/ISO17799

2.以下哪个标准涉及风险评估要求？ A

A. ISO27001/ISO17799

B. ISO14000

C. ISO9000

D. ISO15408

3. ISO17799:2005增加了以下那部分内容？ B

A. 资产管理

B. 信息安全事件管理

C. 人力资源安全

D. 信息系统得获取、开发和维护

4. 以下关于信息安全资产的答案哪个是正确的？ D

A. 人员是资产

B. 公司形象是资产

C. 数据是资产

D. A、B、C都是

5. 残余风险是风险处理后残留的风险，我们不需要对其进行监控。这种说法？B

A. 正确的

B. 错误的

6.  为了工作方便和工作效率，在内审时内审员可以审核自己的工作，这种做法是? A

A.错误的

B. 正确的

7. 在策略生命周期中，以下哪个是正确的：(   D     )

A. 需求分析、制定、发布、推行、审核、废除

B. 制定、发布、推行、审核、修订、废除

C. 需求分析、制定、发布、推行、审核、修订

D. 需求分析、制定、发布、推行、审核、修订、废除

8. 与信息资产有关的弱点或安全隐患对资产构成威胁，这种说法是？ A

A.错误的

B. 正确的

9. 风险评估主要包括以下哪几个方面的评估？ B

A. 资产、威胁、弱点

B. 资产及价值、威胁、弱点、已有控制措施

C. 资产及价值、威胁、弱点

D. 资产、威胁、弱点、已有控制措施

10．在BS779-2:2002版中，下列对P-D-C-A过程的描述错误的是？ D

A. P代表PLAN,即建立ISMS环境&风险评估

B. D代表DO ,即实现并运行ISMS

C. C代表CHECK,即监控和审查ISMS

D. A代表ACT,即执行ISMS

11．ISO/IEC 17799源于以下哪个标准？ A

A. BS7799-1

B. BS7799-2

C. BS7799-3

D.GB 7799

12．ISMS指的是什么？ D

A.信息安全管理

B.信息系统管理体系

C.信息系统管理安全

D.信息安全管理体系

13．以下哪个不属于信息安全的三要素之一？ C

A. 机密性

B. 完整性

C.抗抵赖性

D.可用性

14． ISMS文档体系中第一层文件是？ A

A.信息安全方针政策

B.信息安全工作程序

C.信息安全作业指导书

D.信息安全工作记录

15．在信息系统安全中，资产所具备的风险由以下哪两种因素共同构成的？ C

A．攻击和脆弱性

B．威胁和攻击

C．威胁和脆弱性

D．威胁和破坏

6. 移动存储介质的管理和使用应防止（ ）。

A. 信息失效 B. 病毒危害 C. 公私混用 D. 遗失、被盗

7. 计算机机房装修材料应符合GB 50016《建筑设计防火规范》，选择（ ）。

A. 难燃、非燃材料 B. 防潮、防起尘材料

C. 吸音、抗静电材料 D. 防辐射材料

8. 电源是计算机网络系统的命脉，计算机机房后备电源应选择( )。

A. UPS B. 发电机 C. 蓄电池 D. 干电池

9. 计算机机房应安装( )。

A. 门禁、影像监控系统 B. 温度、湿度监控系统

C. 防火、 防水、防潮系统 D. 以上都是

10. 窃听技术是在窃听活动中使用的窃听设备和窃听方法的总称。不用中继技术窃听距离最远的技术是( )。

A. 谐波无线窃听 B. 微波窃听 C. 激光窃听

D. 电话窃听 E. 定向麦克风 F. 外墙音频放大器

11. 窃照装置也越来越多样化、微型化，下面（ ）属于窃照装置。

A. 可伸缩光学窥镜 B. 电视窥视录像机

C. 微光电视录像机 D. 光纤窥视系统

**二、案例分析**

1、查某公司设备资产，负责人说台式机放在办公室，办公室做了来自环境的威胁的预防；笔记本经常带入带出，有时在家工作，领导同意了，在家也没什么不安全的。

主要观点：A 9.2.5  组织场所外的设备安全  应对组织场所的设备采取安全措施，要考虑工作在组织场所以外的不同风险

2、某公司操作系统升级都直接设置为系统自动升级，没出过什么事，因为买的都是正版。

主要观点：A 12.5.2 操作系统变更后应用的技术评审  当操作系统发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。

3、创新公司委托专业互联网运营商提供网络运营，供应商为了提升服务级别，采用了新技术，也通知了创新公司，但创新认为新技术肯定更好，就没采取任何措施，后来因为软件不兼容造成断网了。

主要观点：A 10.2.3 第三方服务的变更管理 应管理服务提供的变更，包括保持和改进现有的信息安全策略、规程和控制措施，并考虑到业务系统和涉及过程的关键程度及风险的评估。

4、作为企业的CIO，请就本单位的人员使用、升迁或离职、新员工招聘谈谈如何进行信息安全管理。

二、简答题

1、ISO/IEC 17799的十一个管理要项（十一个范畴）是什么？

安全方针

信息安全组织

资产管理

人力资源安全

物理与环境安全

通信和运作管理

访问控制

信息系统的获取、开发与维护

信息安全事件管理

业务连续性管理

符合

2、请简要描述信息安全风险的相关要素？

资产：是任何对组织有价值的东西

威胁：可能导致信息安全事故和组织信息资产损失的活动，威胁是利用脆弱性来造成后果

脆弱性：与信息资产有关的弱点或安全隐患，脆弱性本身并不对资产构成危害，但是在一定条件得到满足时，脆弱性会被威胁加以利用来对信息资产造成危害。

安全措施：可以降低威胁利用脆弱性导致安全事件发生的可能性。

安全风险：是指一种特定的威胁利用一种或一组脆弱性造成组织的资产损失或损害的可能性。

**知识点：**

1. 《信息系统安全等级保护测评准则》将测评分为安全控制测试和系统整体测试两个方面。

2. 安全扫描可以弥补防火墙对内网安全威胁检测不足的问题。

3. 1994年2月18日国务院发布《计算机信息系统安全保护条例》。

4. 安全审计跟踪是安全审计系统检测并追踪安全事件的过程。

5. 环境安全策略应当是简单而全面。

6. 安全管理是企业信息安全的核心。

7. 信息安全策略和制定和维护中，最重要是要保证其明确性和相对稳定性。

8. 许多与PKI相关的协议标准等都是在X.509基础上发展起来的。

9. 避免对系统非法访问的主要方法是访问控制。

10. 灾难恢复计划或者业务连续性计划关注的是信息资产的可用性属性。

11. RSA是最常用的公钥密码算法。

12. 在信息安全管理进行安全教育和培训，可以有效解决人员安全意识薄弱。

13. 我国正式公布电子签名法，数字签名机制用于实现抗否认。

14. 在安全评估过程中，采取渗透性测试手段，可以模拟黑客入侵过程，检测系统安全脆弱性。

15. 病毒网关在内外网络边界处提供更加主动和积极的病毒保护。

16. 信息安全评测系统CC是国际标准。

17. 安全保护能力有4级：1级－能够对抗个人、一般的自然灾难等；2级－对抗小型组织；3级－对抗大型的、有组织的团体，较为严重的自然灾害，能够恢复大部分功能；4级－能够对抗敌对组织、严重的自然灾害，能够迅速恢复所有功能。

18. 信息系统安全等级分5级：1－自主保护级；2－指导保护级；3－监督保护级；4－强制保护级；5－专控保护级。

19. 信息系统安全等级保护措施：自主保护、同步建设、重点保护、适当调整。

20. 对信息系统实施等级保护的过程有5步：系统定级、安全规则、安全实施、安全运行和系统终止。

21. 定量评估常用公式：SLE（单次资产损失的总值）＝AV（信息资产的估价）×EF（造成资产损失的程序）。

22. SSL主要提供三方面的服务，即认证用户和服务器、加密数据以隐藏被传送的数据、维护数据的完整性。

23. 信息安全策略必须具备确定性、全面性和有效性。

24. 网络入侵检测系统，既可以对外部黑客的攻击行为进行检测，也可以发现内部攻击者的操作行为，通常部署在网络交换机的监听端口、内网和外网的边界。

25. 技术类安全分3类：业务信息安全类（S类）、业务服务保证类（A类）、通用安全保护类（G类）。其中S类关注的是保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改；A类关注的是保护系统连续正常的运行等；G类两者都有所关注。

26. 如果信息系统只承载一项业务，可以直接为该信息系统确定安全等级，不必划分业务子系统。

27. 信息系统生命周期包括5个阶段：启动准备、设计/开发、实施/实现、运行维护和系统终止阶段。而安全等级保护实施的过程与之相对应，分别是系统定级、安全规划设计、安全实施、安全运行维护和系统终止。

### 信息安全管理体系审核员练习题-简述题-2015

简述题

**1、审核员在某公司审核时，发现该公司从保安公司聘用的保安的门卡可通行公司所有的门禁。公司主管信息安全的负责人解释说，因保安负责公司的物理区域安全，他们夜里以及节假日要值班和巡查所有区域，所以只能给保安全权限门卡。审核员对此解释表示认同。如果你是审核员，你将如何做？**

答：应根据标准GB/T 22080-2008条款A.11.1.1审核以下内容：

（1）是否有形成文件的访问控制策略，并且包含针对公司每一部分物理区域的访问控制策略的内容？

（2）访问控制策略是否基于业务和访问的安全要素进行过评审？

（3）核实保安角色是否在访问控制策略中有明确规定？

（4）核实访问控制策略的制定是否与各物理区域风险评价的结果一致？

（5）核实发生过的信息安全事件，是否与物理区域非授权进入有关？

（6）核实如何对保安进行背景调查，是否明确了其安全角色和职责？

**2、请阐述对GB/T 22080中A.13.2.2的审核思路。**

答：（1）询问相关责任人，查阅文件3-5份，了解如何规定对信息安全事件进行总结的机制？该机制中是否明确定义了信息安全事件的类型？该机制是否规定了量化和监视信息安全事件类型、数量和代价的方法和要求，并包括成功的和未遂事件？

（2）查阅监视或记录3-15条，查阅总结报告文件3-5份，了解是否针对信息安全事件进行测量，是否就类型、数量和代价进行了量化的总结，并包括成功的和未遂事件。

（3）查阅文件和记录以及访问相关责任人，核实根据监视和量化总结的结果采取后续措施有效防止同类事件的再发生。