### 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。

**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

4. 《信息安全国家学说》是（　C　）的信息安全基本纲领性文件。

A. 法国　　B. 美国　　C. 俄罗斯　　D. 英国

注：美国在2003年公布了《确保网络空间安全的国家战略》。

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

8. 在PDR安全模型中最核心的组件是（　A　）。

A. 策略　　B. 保护措施　　C. 检测措施　　　D. 响应措施

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。

15. 公钥密码基础设施PKI解决了信息系统中的（　A　）问题。

A. 身份信任   B. 权限管理   C. 安全审计   D. 加密

注：PKI（Public Key Infrastructure,公钥密码基础设施)，所管理的基本元素是数字证书。

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

**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。

### 信息安全管理体系国家注册审核员培训班考试试题-2015

 一、选择题(每题1分，共l0分)

 ( c )1．信息安全中的可用性是指\_\_\_\_\_\_\_

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

 ( a )2．审核证据是指\_\_\_\_\_\_\_\_

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

 ( abcd )3．\_\_\_\_\_\_    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

( abc )4．管理体系是指\_\_\_\_\_\_

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

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

 ( abcd )6．在信息安全管理体系\_\_\_\_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

 ( b )7．风险评价是指\_\_\_\_\_\_

 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

(a  )8．可使用\_\_\_\_\_\_\_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

( abc )9．现状不符合文件是指\_\_\_\_\_\_

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

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

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

二、判断题(每题1分，共10分)

你认为正确的在(  )中划“√”，错误的划“x”。

( 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。

三、填空题(每题1分，共5分)

  指出IS027001：2005标准中适用于下述情景的某项条款，请将条款号填在横线上。

  1．“信息安全管理部的员工根据风险评估的结果，正在选择适当的控制措施。” 适用于这一情况的条款是——

  2．“某公司规定无论离职或调职，员工的原有系统访问权一律撤销。”    适用于这一情况的条款是——

  3．“某公司在其机房内贴了一张行为准则，员工在机房内工作时必须遵守。”

    适用于这一情况的条款是——

  4．“公司重要服务器的操作记录中没有任何管理员操作的记录。”

    适用于这一情况的条款是——

  5．“某公司的信息系统中使用了密码手段来保障其信息安全，但该公司的相关工作人员对我国密码方面的法律法规一无所知。”

    适用于这一情况的条款是\_\_\_\_\_\_

四、问答题(1—3题每题5分，共15分；4．5题每题15分，共30分；共45分)

 1．什么是信息安全?组织的信息安全要求分为哪几类?并简要说明。

2．ISO／IEC 27001：2005附录A所列出的控制措施中，哪些条款体现了“管理者作用”，至少举出3条控制措施，并简要说明。

3．审核组进入审核现场后，通常会有哪些会议?各有什么作用?会议主持人一般由谁担任?

4．如果某软件开发公司涉及软件外包业务，请列出在软件外包的过程中所涉及的风险，并

从ISO／IEC 27001：2005附录A控制措施列表中选择适当的控制措施，作简要说明。

5．如何依据ISO／IEC 27001：2005审核A．10．7，组织应防止资产遭受未授权泄露、修改、

移动或销毁以及业务活动的中断

五、案例分析题(每题10分，共30分)

请根据所述情况判断：如能判断有不符合项，请写出不符合ISO/2700l：2005标准的条款号、内容和严重程度，并写出不符合事实，如提供的证据不能足以判断有不符合项时，请写出进一步审核的思路。

判分标准：不符合条款2分，不符合标准的内容3分，不符合事实3分，不符合的严重程度2分。

1．审核员在看到某公司的意识及技能培训计划后，询问某公司工作人员对信息安全管理体系的认识，该工作人员回答，由于前段时间一直出差在外，所以还没有时问学习相关的体系文件。

2．审核员询问公司办公系统中某机器的操作系统升级情况时，使用人员说，我们使用的所有软件都是正版的，所以我在使用时直接设置为操作系统自动更新了，而且一直也没出现过什么问题，对业务没有任何影响。

3．审核员在某公司信息安全部看到几份安全事故处理报告，原因栏写的都是感染计算机病毒，工作人员说，我们已经严格规定了防病毒软件的使用及升级周期，但还是没有效果。

### 信息安全管理体系审核员练习题-简单题和案例分析题-2015

一、简答

**1.内审不符合项完成了30/35，审核员给开了不符合，是否正确？你怎么审核？**

**[参考]不正确。应作如下审核：**

（1）询问相关人员或查阅相关资料（不符合项整改计划或验证记录），了解内审不符合项的纠正措施实施情况，分析对不符合的原因确定是否充分，所实施的纠正措施是否有效；

（2）所采取的纠正措施是否与相关影响相适宜，如对业务的风险影响，风险控制策略和时间点目标要求，与组织的资源能力相适应。

（3）评估所采取的纠正措施带来的风险，如果该风险可接受，则采取纠正措施，反之可采取适当的控制措施即可。

综上，如果所有纠正措施符合风险要求，与相关影响相适宜，则纠正措施适宜。

**2、在人力资源部查看网管培训记录，负责人说证书在本人手里，培训是外包的，成绩从那里要，要来后一看都合格，就结束了审核，对吗？**

[参考]不对。

应按照标准GB/T 22080-2008条款5.2.2 培训、意识和能力的要求进行如下审核：

（1）询问相关人员，了解是否有网管岗位说明书或相关职责、角色的文件？

（2）查阅网管职责相关文件，文件中如何规定网管的岗位要求，这些要求基于教育、培训、经验、技术和应用能力方面的评价要求，以及相关的培训规程及评价方法；

（3）查阅网管培训记录，是否符合岗位能力要求和培训规程的规定要求？

（4）了解相关部门和人员对网管培训后的工作能力确认和培训效果的评价，是否保持记录？

（5）如果岗位能力经评价不能满足要求时，组织是否按规定要求采取适当的措施，以保证岗位人员的能力要求。

**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。

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。

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。

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、查某公司信息安全事件处理时，有好几份处理报告的原因都是感染计算机病毒，负责人说我们严格的杀毒软件下载应用规程，不知道为什么没有效，估计其它方法更没用了。

8.2纠正措施

5、查看 web服务器日志发现，最近几次经常重启，负责人说刚买来还好用，最近总死机，都联系不上供应商负责人了。

A 10.2.1 应确保第三方实施、运行和保持包含在第三方服务交付服务交付协议中的安全控制措施、服务定义和交付水准。

### 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。

### ISO27001信息安全管理体系审核员培训测试-2015

一、以下对于信息安全管理体系的叙述，哪个个是不正确的？

A.只规范公司高层与信息安全人员的行为；

B.针对组织内部所使用的信息，实施全面性的管理；

C.为了妥善保护信息的机密性、完整性和可用性；

D.降低信息安全事件的冲击至可承受的范围；

E.分为PDCA（计划—执行—检查—行动）四大部份，循环执行，不断改进。

二、以下对于PDCA（计划—执行—检查—行动）的叙述，哪个是正确的？

A.其中的重点在于P（计划）；

B.依据PDCA的顺序顺利执行完一次，即可确保信息安全；

C.需依据管理层审查结果采取矫正与预防措施，以达到持续改进的目的；

D.如果整体执行过程中C（检查）的过程过于繁复，可予以略过；

E.以上皆非。

三、下列那个项目不属于ISO27001认证标准所涵盖的十一个管理要项？

A.信息安全政策；

B.组织安全；

C.人员安全；

D.复杂性；

E.访问控制。

四、下列对于风险的叙述，哪个是正确的？

A.风险分析：针对无法改善的风险进行分析；

B.风险管理：列出所有可能存在的风险清单；

C.风险评估：把所估计的风险与已知的风险标准作比较，以决定风险的重要性；

D.风险处理：为了将风险降为零风险所采取的行动；

E.可接受风险：可接受进行改善的风险。

五、以下哪项符合信息安全管理体系有关“文件记录控制”的要求？

A.文件都必须电子化；

B.信息安全管理体系所需的文件仅需保护，但无须控制；

C.所有文件应依据信息安全管理体系的政策要求在需要时即可供被授权人取用；

D.文件纪录必须全部由一人保管；

E.为提供信息安全管理体系有效运作的证据所建立之纪录不属于管制范围。

六、对于“信息安全管理体系”，下列哪些不属于管理层的责任？

A.提供信息安全管理工作的必要资源；

B.决定可接受风险的等级；

C.定期举行相关教育训练，增进员工信息安全的认知；

D.为信息安全系统购买保险；

E.建立一份信息安全政策。

七、以下针对信息安全系统审计的叙述，哪个是不正确的？

A.审计方案应予以事先规划；

B.目的在于确保信息安全管理体系的控制目标与控制措施是否有效地实施与维持；

C.基于对业务的了解，应由各部门主管审计其所负责的业务；

D.对于审计结果应有适当的跟进措施；

E.审计人员的遴选与审计的执行，应确保审计过程的客观性与公正性。

八、以下对于信息安全管理体系改进的叙述，哪个是不正确的？

A.改进的目的在于确认信息安全管理系统的有效性；

B.为了防止不符合事项再度发生，应将该事项从信息安全管理体系中移除；

C.包含矫正措施与预防措施；

D.应在信息安全管理体系中制定相应的文件化程序；

E.应决定相关措施，以消除未来不符合信息安全管理体系要求的事项。

九、以下对于“安全方针”的叙述，哪个是不正确的？

A.管理层应设定一个明确的政策方向，展现对信息安全的支持与承诺；

B.安全方针应以适当方式向所有员工公布与宣导；

C.安全方针应有专人依据规定的审核过程对其进行维护与审核；

D.安全方针一经确定即无法随意修改；

E.方针应说明组织管理信息安全的方法。

十、以下对于“信息安全组织”的叙述，哪个是不正确的？

A.其目标为在组织中管理信息安全；

B.个别资产的保护责任及执行特定安全程序的责任应明确划分；

C.应参考信息安全专家的建议；

D.应减少与其它组织间的合作；

E.需有独立的信息安全审计。

十一、针对“第三方存取”与“外包作业”的叙述，哪个是正确的？

A.为了降低风险，应减少「第三方存取」与「外包作业」；

B.第三方存取组织信息处理设施的风险应予评估，并实施适当的安全控制措施；

C.将信息处理责任外包时，信息安全的责任也随之转嫁；

D.应限制外包单位不得使用组织的任何信息设备；

E.由于已签订外包合同，对于第三方存取组织的信息处理设施无须控制。

十二、以下对于“资产分类及控制”之叙述，哪个是不正确的？

A.所有主要的信息资产应由高级管理人员负责保管；

B.应制作所有与每一信息系统相关重要资产的清册并进行维护；

C.应制订一套与组织采用的分类方式相符的信息标识和处理流程；

D.信息分类与相关保护控制措施应考虑企业共享或限制信息的需求；

E.其目标在于维护组织资产并给予适当的保护。

十三、以下对于“人力资源安全”的叙述，哪个是不正确的？

A.组织信息安全方针中规定的安全角色与职务应在工作职责中予以文件化；

B.组织内所有员工及相关第三方的用户皆应接受适当的信息安全教育训练；

C.目标在于确保员工的人身安全，避免发生意外；

D.正式员工、承包商及临时工在申请工作时即应进行背景调查；

E.员工应签署保密协议，作为任用的首要条件和限制的一部分。

十四、员工察觉“安全及失效事件”发生时，应立即采取何种行动？

A.分析事件发生的原因；

B.尽快将事件掩盖过去；

C.修正信息安全目标；

D.查阅信息安全相关文件；

E.遵循适当的管理途径尽快通报。

十五、以下对于“安全区域”的说明，哪个是不正确的？

A.其目标是避免营运场所及信息遭未经授权存取、损害与干扰；

B.划设为安全区域的场所已有适当控管，可容许任何人进出；

C.应设立安全区域，以提供特殊安全需求；

D.在安全区域内工作时应采取额外的控制措施及指引，以强化该区域的安全性；

E.装卸区应予管制，若可能，应与信息处理设施隔离，避免遭未授权进入。

十六、以下对于“设备安全”的相关行为，哪个是不适当的？

A.应保护设备降低来自环境的威胁及灾害；

B.保护设备不受电力故障及其他电力异常影响；

C.保护传送数据或支持信息服务的电源与通讯缆线，以防止窃听或破坏；

D.设备在报废或再使用前将信息清除；

E.设备一律禁止携出组织外使用。

十七、以下何种行为不符合“通信和操作安全”的要求？

A.信息处理设施与系统的变更应予控制；

B.职务与责任范围应予区分，以降低信息或服务遭未授权修改或误用的机会；

C.安全政策所规定的作业程序应制作文件纪录并进行维护；

D.开发与测试工作可在正式生产设备上进行，以降低营运成本；

E.使用外部设施管理服务前，应识别风险并制订适当的控制措施。

十八、下列对于“信息的交换”的叙述，哪个是不正确的？

A.组织间交换信息与软件的行为应有协议或合约规范；

B.应制定电子邮件使用政策，严格执行控管；

C.使用网络及时通讯软件（如MSN）进行文件传送以便于实现传送的方便性及隐密性；

D.重要信息对外公开前应有正式授权程序，且该信息的完整性应予保护；

E.运送的储存媒体应予保护，防止未经授权遭存取。

十九、下列对于“用户访问控制”的叙述，哪个是不正确的？

A.应制定正式用户注册及注销流程；

B.特殊权限的分配与使用应受限制与控管；

C.要确保信息系统的访问权限被恰当地授权、配置及维护；

D.为减少账号个数，降低日常作业成本，可采多人共享一组账号密码的方式；

E.管理层应定期执行正式程序复核用户访问权限。

二十、下列行为哪个不符合“网络访问控制”的安全需求？

A.网络应有控制措施，将信息服务、用户及信息系统群组分离；

B.用户网络联机能力应仅限于共享网络；

C.组织应对其使用的所有网络服务的安全特性提供一份清楚说明的文件；

D.远程使用者的存取应有身份鉴别；

E.为便利用户，应设置开放的网络环境，以确保用户可直接存取任何他所想使用的服务。

二一、对于“监控系统”的存取与使用，下列哪个是正确的？

A.监控系统所产生的记录可由用户任意存取；

B.计算机系统时钟应予同步；

C.只有当系统发生异常事件及其他安全相关事件时才需进行监控；

D.监控系统投资额庞大，并会影响系统效能，因此可以予以暂时省略；

E.以上皆非。

二二、以下各项行为，哪个不能确保“应用系统的安全”？

A.输入、输出数据应进行确认；

B.对于有保护消息内容完整性的安全要求的应用程序，应采用消息鉴别机制；

C.要有适当的审计记录或活动日志；

D.系统内应有确认检查机制，以检测所处理数据的完整性；

E.为加快数据传输时的速度，降低系统反应时间，任何数据皆可使用明码传输。

二三、下列哪项不是维护“开发和支持过程中的安全”的方法？

A.应阻止用户修改软件包，必要的修改应严格管制；

B.应用系统若有变更，应进行适当审核与测试；

C.应采取正式变更管理程序以严格控制变更作业的实施；

D.软件应尽量采用自行开发避免外包或采购；

E.软件的采购应注意其是否内藏隐密通道及特洛依木马程序。

二四、为确保“业务连续性管理”，以下哪些行为应该加以避免？

A.应分析各种灾难、安全缺失和损失服务对业务所可能产生的后果；

B.全组织连续营运措施的制订与维护，有明确管理的过程；

C.应等待企业营运过程发生中断或失效时，再来制订相关的策略计划；

D.应维持单一营运持续计划的框架，以确保所有计划皆一致；

E.营运持续计划应定时测试，并通过定期审查加以维护。

二五、以下对于信息安全管理体系中“符合性”的叙述，哪个是不正确的？

A.清楚识别所有与信息系统有关的法规；

B.组织重要记录应予文件化后进行保护；

C.避免使用具有知识产权的专利软件产品；

D.要保护个人信息的数据与隐私；

E.信息系统的管理要依据行政命令、法律规章或合同的安全要求。

### 信息技术服务管理体系审核员练习-2015

一．选择题（请选出最佳答案，每题2分，共20分）

1.01 修改SLA和支持文件应属于哪个流程的一部分：

a）变更管理

b）配置管理

c）发布管理

d）业务持续性和可用性管理

e）以上都不是

1.02 服务目录不包括以下哪个信息。

服务名称

服务成本

目标，如：安装一个打印机的回应时间，恢复一个重大事故的时间等

联络点

以上都是

1.03以下哪个不是IT服务管理的工具

交互语音应答系统

安全服务

自学知识库

网络管理工具

包含配置管理项的excel表

1.04事件管理程序运行一段时间后，为反应事件升级新的途径，事件经理想对事件管理程序文件进行修改，并得到 IT 服务管理委员会的同意，在这个过程中，审核员要优先考虑以下哪方面的审核：

能力、意识和培训

文件控制

事件管理流程的设计更改

事件管理流程与其他流程的接口

1.05哪些内容应包括在对员工进行的IT服务培训中

服务管理方针策略

事故处理

SLA

怎样使用服务台工具

以上都是

1.06 “在变更之前应评估控制措施变更的影响”是哪个流程中提到的。

配置管理

信息安全管理

变更管理

计划和实施新的或变更的服务

以上都不是

1.07认证一个组织的ITSMS是依据：

ISO/IEC20000-1:2011

ISO/IEC20000-2:2005

ISO 19011:2002

以上都是

以上都不是

1.08风险分析是

指导和控制一个组织的风险的联合行动

选择和实施测量机制以修改风险的处置决定。

接受风险的决定

系统化的使用信息以识别风险的来源并估计风险的大小

以上都不是

1.09  根据ISO20000-1的要求，下列那个活动需要一个文件化的程序。

管理评审

管理责任

改进IT服务管理体系

纠正措施

以上都不是

1.10落实资金、预算、角色、责任、文件化和维护方针策略、计划、程序和定义等是PDCA方法的那个阶段

策划

实施

检查

改进

以上都是

二．简答题（每个问题5分，共20分）

2.01列出至少5个实施IT服务管理体系对组织的好处（5分）

2.02 列出至少五个期望 ISO20000-1审核小组所具备的能力。（5分）

2.03举出至少5个内部审核员在准备内审计划时需要获得的信息（5分）

2.04作为审核员，当你对防火墙策略变更进行审核时，应查找哪些客观证据？

三．问答题

请在空白处，写出下面两个问题的详细答案，适当时，写出ISO20000-1相关的条款。每个问题10分。

3.01 清楚解释被审核方于对内审所提出的不符合事项通常所采取的纠正措施的步骤（由开始识别到不符合事项至关闭此不符合事项）。并鉴别各阶段谁应负责（例：审核员或被审核方）

3.02审核员正在计划给一个提供灾备服务的组织进行ISO20000-1 内部审核，识别至少包含5个审核要项的检查表来审核配置管理过程。

四．案例分析

以下是三个事件是在ITSMS内审审核时发现的，他们包含了可能产生不符合事项（需要书写不符合事项的报告）的情况，仔细考虑每种情况，然后采取下面的某个措施。

如果你认为有足够的不符合的客观证据，应完成一个不符合事项报告，并将不符合分类为重大（严重）不符合或轻微（一般）不符合

如果你不认为有足够的客观证据提出一个不符合报告，你需要在报告下面的空白处陈述自己的理由，你必须同时陈述审核员下一步需要做什么。

4.01事件1

在对一个内部IT服务部门进行第三方审核时，发现不存在《连续性计划》。经理对审核员解释说，连续性管理是与可用性管理的流程写在一起的，《可用性管理计划》里已经描写了在发生火灾时的应对措施，在去年9月份作了测试和演练。

4.02 事件2

在审核一个数据处理中心时，检查培训记录时发现很多的培训已完成，但是没有发现出现针对服务管理的培训课程完成的证据，处理中心的经理解释正式的培训要延期到下一年。因为培训的财务经费困难，一个系列的服务培训已经通过网络进行而且已经跟所有人讨论过了。

4.03 事件3

在对一个IT 服务机构的ISO20000-1审核时，发现有一个有关服务质量的客户投诉，该投诉已经由投诉经理处理，并作了记录。与投诉相关的一项技术问题的处理。转给了问题管理流程，还没有得到反馈；当审核员询问问题管理经理这个问题的处理状态时，问题经理回答，因为问题比较复杂，正在处理过程中，当审核员要求察看处理状态的记录时，问题经理说，不需要记录，因为处理问题的几位同事都很清楚当前的状态。

### 信息技术服务管理体系审核员练习模拟题

一、 选择题（共30题，每题2分，总60分）

1) 下面哪句话最恰当描述了IT服务管理？

A. 经济有效地管理IT服务的质量

B. 根据ITIL最佳实践进行IT基础设施的管理工作

C. 以流程的方式管理IT基础设施。这种方式可让IT组织能够以专业的方式为客户提供IT产品和服务

D. 促进更多的人了解IT服务

2) IT服务管理是如何改善IT服务的质量的。

A. 以正式的内部、外部客户以及供应商的服务协议

B. 定义服务级别普遍适用的标准

C. 提高IT组织中所有员工的客户关注程度

D. 计划、实施、管理一系列流程以提供IT服务

3) 硬件、系统和应用软件以及数据通讯设施都是IT基础架构（IT infrastructure）的组成部分。下面哪些组件也可以被视为IT基础架构的一部分？

1 程序    2 文档     3 人员

A. 1和2

B. 1和3

C. 2和3

D. 1，2和3

4) 事件管理流程可以从哪份文档获得有关何时有必要将问题升级和将问题升级给谁等方面的信息？

A. 服务改进计划

B. 服务目录

C. 组织结构图

D. 服务级别协议

5) 考虑下列说法：

1. SLA应该定义协议双方的角色和职责

2. 对SLA的实现情况应该进行监控，定期制作服务级别报告并报送相关人员

3. 在SLA签订之前应该对支撑合同进行评审

A. 没有一个是正确的

B. 1和2是正确的

C. 2和3是正确的

D. 上述三个说法都是正确的

6) 在某个保险公司里，由于电力的中断导致局域网和所有PC都宕机了。因此，该公司的业务受理系统和理赔系统都不能正常使用。一个小时后，电力中断的故障被解决了，服务也恢复至电力中断之前的状态。该事件对服务提供造成了哪种影响？

A. 影响很小，因为在一个小时内客户就被告知电话通知可以继续办理业务了，并且客户对这种情况表示理解。

B. 影响重大，因为该事件使得正常的服务提供不能实现。这对公司的形象造成了损害。

C. 没有影响，因为所有的数据都可以先记录在纸质文档上并可以在电力恢复后在录入系统。

D. 影响非常小，因为该事件是由电力故障而不是硬件或软件错误引起的。

7) 以下哪一项是IT服务持续性管理流程的典型活动？

A. 通知终端用户有关系统故障方面的情况

B. 将后备方案（Fallback Arrangement）文档化

C. 提供可用性方面的报告

D. 确保配置项始终是最新的

8) 某钢铁公司被竞争对手兼并。IT部门以及两个公司的IT基础架构需要整合，IT基础架构整合后运行应用程序所需要的磁盘空间将由下列哪项流程决定。

A. 可用性管理

B. 能力管理

C. 计算机操作管理

D. 发布管理

9) 关于IT服务持续性计划，某个灾难的严重程度取决于：

A. 灾难持续的天数

B. 恢复灾难可用的人员数量

C. 灾难的类型，如洪水、火灾等

D. 对客户业务的影响

10) 因对信息系统的依赖逐渐增强，某房地产公司要求确保系统运行发生中断后仍可获得IT服务。下面哪个流程可提供这样的服务。

A. 可用性管理

B. 持续性管理

C. 服务级别管理

D. 服务管理

11) 下面哪些属于可用性管理的首要职责？

1. 计划在SLA中约定的IT服务的可用性并进行监控

2. 就SLA中的可用性级别与客户进行谈判

3. 记录不可用事件的详细情况

4. 提出变更以预防有损可用性的故障

A. 1和2

B. 3和4

C. 所有的都正确

D. 1和4

12) 可用性百分率的计算公式为：

A. （宕机时间\*100）/约定服务时间

B. （约定服务时间\*100）/宕机时间

C. （（约定服务时间-宕机时间）\*100）/约定服务时间

D. 约定服务时间/（约定服务时间-宕机时间）

13) 某企业针对某项特定的IT服务没有任何持续性计划，下面哪个将是合适的理由？

A. IT部门不具备开发持续性计划的技巧和能力

B. IT部门业务灾难的风险是很少的

C. 业务方的相关人员没有时间参与开发持续性计划

D. 在进行业务影响评估之后所作出的管理决策

14) 概念不属于IT服务的预算及核算管理？

A. 预算编制

B. 计费

C. 采购

D. 核算

15) 网络部门与外部组织就提供内部服务方面达成协议，将在何处说明此协议？

A. 运营级别协议

B. 服务级别协议

C. 服务级别需求

D. 支持合同

16) 下面关于IT服务的预算及核算管理表述中哪一项是不正确的？

A. IT服务财务经理需要负责确认和计量IT成本并为所提供的IT服务制定价格

B. 为了能够建立IT服务预算和核算体系，应该先签订SLA和OLA

C. 只有当对客户使用的服务进行计费时才有可能提高成本意识

D. IT服务的预算及核算管理必须在建立成本核算模型之前与客户就收费问题达成协议

17) 哪个流程负责为需求中的IT服务的购买事宜制定（长期）计划？

A. 可用性管理

B. 能力管理

C. 配置管理

D. 服务级别管理

18) 保密性是安全管理流程要实现的目标之一。以下哪项正确地说明了“保密性”这个术语的含义？

A. 对数据的保护以防止未经授权的访问和使用

B. 随时访问数据的能力

C. 验证数据正确性的能力

D. 数据的正确性

19) 你是某个IT组织中的服务台人员。有一个用户呼叫电话说它的某个终端设备不能使用了。请问这是一个？

A. 事件

B. 已知错误

C. 问题

D. 变更请求

20) 一个良好的事件管理流程将可以：

A. 确保错误的修改像处理紧急变更一样进行处理

B. 快速地诊断事件发生的潜在原因

C. 在事件发生后尽快地恢复正常的服务运作

D. 以上三项都是

21) 下列哪项活动属于事件管理的职责？

A. 变更在基础架构中的应用

B. 检测事件产生的原因

C. 识别事件背后的潜在问题

D. 事件的排除

22) 由于产品本身的问题，用户现有的声卡被一块新的声卡替换。为方便以后参考，需对这块由另外一个制造厂商生产的新声卡进行登记。请问这项工作应由哪个流程负责执行？

A. 变更管理

B. 配置管理

C. 事件管理

D. 问题管理

23) “已知错误（Known Error）”与“问题”在ISO20000中的不同之处表现在哪些方面？

A. 导致已知错误的潜在原因是已知的，而导致问题的潜在原因是未知的

B. 已知错误与IT基础架构中出现的错误有关，而问题则与其无关

C. 已知错误通常某个事件，而问题则不完全是这样的

D. 对问题而言，与其有关的配置项已经发现和确认，而与已知错误有关的配置项通常仍未发现

24) 以下哪项活动属于主动问题管理？

A. 处理变更请求（RFC）

B. 进行趋势分析，发现潜在的事件的问题

C. 跟踪所有的事件和服务中断

D. 尽量减少由于IT环境的变更而造成的服务中断

25) 某公司财务管理数据只能提供给授权的用户，安全管理采取措施来确保这点。这样做可以确保数据的哪个方面的安全性得到保证？

A. 可用性

B. 完整性

C. 稳定性

D. 机密性

26) 一个用户向服务台抱怨说，当他使用某个应用系统的时候，有一个错误总是反复地出现，从而导致网络连接的中断。下面哪个流程负责检测该错误产生的原因？

A. 事件管理

B. 网络管理

C. 问题管理

D. 系统开发

27) 当某个软件包的最新版本被安装到某个台式机时，它可能会影响其它软件包。哪个流程负责检查和判断其它软件包是否有必要测试或者重新安装？

A. 变更管理

B. IT服务持续性管理

C. 问题管理

D. 发布管理

28) 以下哪项变更必须经变更管理流程批准后才能实施？

A. 用户录入数据到数据库中

B. 改变密码

C. 给系统增加一位新用户

D. 将打印机从二楼移到三楼

29) 配置管理数据库（CMDB）中的哪个属性有助于查明某个时刻的哪些配置项正在进行维护？

A. 购买日期

B. 责任人（Owner）

C. 位置

D. 状态

30) 下列哪项是配置基线？

A. 配置管理数据库中的标准配置

B. 标准配置项的描述

C. 以交付的一系列配置项

D. 有关一项产品或服务的“快照”，以作为配置审计和变更回撤的基准

二、 简单题（共2题，每题5分，总10分）

1. 请说明ITSM的定义。

ITSM: 是一套面向过程、以客户为中心的规范的管理方法，它通过集成IT服务和业务，协助企业提高其IT服务提供和支持能力。

2. 请描述在贵单位实施ISO20000的意义。

实施ISO20000能提高公司整体效益

就服务质量和服务承诺与业务及供货商达成一致，建立和业务及供货商统一的沟通平台（服务台)；达到相关利益方均满意的IT服务管理目标；

进一步提高IT服务的可用性、完整性和保密性，为业务用户提供高质量的服务；

能够有持续性优化服务流程，提升服务水平，提高业务满意度；

进一步提高项目的可提供性并确保如期交付；

从总体上提高企业IT投资的报酬率，提升企业的综合竞争力；

建立IT部门一整套行之有效的持续改善机制和内控机制；

明确IT管理成本和企业业务战略以及IT战略目标的结合点，完善现有IT服务结构和资源配置，使各项IT资源的运用符合公司业务。

实施ISO20000战略和IT战略目标；

通过建立优化、透明的管理流程和权责的定义，监控管理流程、进行绩效评价；降低IT运营的管理成本和风险；

将现有管理体系和业务流程整合，规范IT部门服务水平，规范工作流程，降低由人员变动导致的风险；

提高IT部门相关员工的专业素质，提高员工的服务能力和工作效率；

提升IT部门整体运作及各部门间沟通的能力。

三、 问答题(共3题,每题10分，总30分)

1. ISO20000要求服务供应商编制服务报告，请问服务报告包括哪些方面的内容。

服务目标以及服务目标针对的对象

服务的内容

总结服务内容

分析服务的趋势

对以后的一个改进措施期望要求

2. 针对ISO20000标准中所包含的13个控制流程，列出您的工作中涉及到的服务流程，并画出其中一个服务流程的流程图。

2.ISO20000要求服务提供商需要实施事件管理、问题管理、变更管理、发布管理、配置管理，请描述这五大流程的目标及它们之间的关系？

目标：

事件管理

在最快的时间内将服务恢复到“正常状态”

问题管理

查找事件或问题产生的根本原因，并彻底解决，以防再次发生

变更管理

控制需要变更的信息并得以处理

发布管理

计划和协调软硬件组件的发布以及进行实际的运行操作

配置管理

更好的管理IT资产的配置组件并提供有效准确的信息

T服务管理培训考试答题卷

**IT服务管理培训考试答题卷**

**一．**    **选择题**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Ｂ | 6 | Ａ | 11 | Ｄ | 16 | Ｂ | 21 | Ｂ | 26 | Ｃ |
| 2 | Ｂ | 7 | Ａ | 12 | Ｃ | 17 | Ｂ | 22 | Ｄ | 27 | Ｄ |
| 3 | Ａ | 8 | Ｂ | 13 | Ｄ | 18 | Ａ | 23 | Ａ | 28 | Ｄ |
| 4 | Ａ | 9 | Ｄ | 14 | Ｃ | 19 | Ａ | 24 | Ｂ | 29 | Ｄ |
| 5 | C | 10 | Ｂ | 15 | Ｂ | 20 | Ｃ | 25 | Ｄ | 30 | Ｄ |

二． 简答题

１．请说明ITSM的定义。

ITSM: 是一套面向过程、以客户为中心的规范的管理方法，它通过集成IT服务和业务，协助企业提高其IT服务提供和支持能力。

２．请描述在贵单位实施ISO20000的意义。

实施ISO20000能提高公司整体效益

就服务质量和服务承诺与业务及供货商达成一致，建立和业务及供货商统一的沟通平台（服务台)；达到相关利益方均满意的IT服务管理目标；

进一步提高IT服务的可用性、完整性和保密性，为业务用户提供高质量的服务；

能够有持续性优化服务流程，提升服务水平，提高业务满意度；

进一步提高项目的可提供性并确保如期交付；

从总体上提高企业IT投资的报酬率，提升企业的综合竞争力；

建立IT部门一整套行之有效的持续改善机制和内控机制；

明确IT管理成本和企业业务战略以及IT战略目标的结合点，完善现有IT服务结构和资源配置，使各项IT资源的运用符合公司业务。

实施ISO20000战略和IT战略目标；

通过建立优化、透明的管理流程和权责的定义，监控管理流程、进行绩效评价；降低IT运营的管理成本和风险；

将现有管理体系和业务流程整合，规范IT部门服务水平，规范工作流程，降低由人员变动导致的风险；

提高IT部门相关员工的专业素质，提高员工的服务能力和工作效率；

提升IT部门整体运作及各部门间沟通的能力。

三． 问答题

1. ISO20000要求服务供应商编制服务报告，请问服务报告包括哪些方面的内容？

服务目标以及服务目标针对的对象

服务的内容

总结服务内容

分析服务的趋势

对以后的一个改进措施期望要求

2.ISO20000要求服务提供商需要实施事件管理、问题管理、变更管理、发布管理、配置管理，请描述这五大流程的目标及它们之间的关系？

目标：

事件管理

在最快的时间内将服务恢复到“正常状态”

问题管理

查找事件或问题产生的根本原因，并彻底解决，以防再次发生

变更管理

控制需要变更的信息并得以处理

发布管理

计划和协调软硬件组件的发布以及进行实际的运行操作

配置管理

更好的管理IT资产的配置组件并提供有效准确的信息

### 信息安全管理培训考核试题

 一、选择题

1.以下哪个是信息安全管理标准？

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. ISO27001/ISO17799

B. ISO14000

C. ISO9000

D. ISO15408

3. ISO17799:2005增加了以下那部分内容？

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？

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。这种说法是？

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.错误的

B. 正确的

7. 在策略生命周期中，以下哪个是正确的：(        )

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.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？

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？

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. BS7799-1

B. BS7799-2

C. BS7799-3

D.GB 7799

12．ISMS指的是什么？

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？

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.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？

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **答案** | **序号** | **答案** | **序号** | **答案** | **序号** | **答案** | **序号** | **答案** |
| **1** | **D** | **2** | **A** | **3** | **B** | **4** | **D** | **5** | **B** |
| **6** | **A** | **7** | **D** | **8** | **A** | **9** | **B** | **10** | **D** |
| **11** | **A** | **12** | **D** | **13** | **C** | **14** | **A** | **15** | **C** |

二、简答题

1、  ISO/IEC 17799的十一个管理要项（十一个范畴）是什么？

2、  请简要描述信息安全风险的相关要素？

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。

### 信息安全管理练习题

**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。

**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

4. 《信息安全国家学说》是（　C　）的信息安全基本纲领性文件。

A. 法国　　B. 美国　　C. 俄罗斯　　D. 英国

注：美国在2003年公布了《确保网络空间安全的国家战略》。

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

8. 在PDR安全模型中最核心的组件是（　A　）。

A. 策略　　B. 保护措施　　C. 检测措施　　　D. 响应措施

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。

15. 公钥密码基础设施PKI解决了信息系统中的（　A　）问题。

A. 身份信任   B. 权限管理   C. 安全审计   D. 加密

注：PKI（Public Key Infrastructure,公钥密码基础设施)，所管理的基本元素是数字证书。

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

**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。