湖南科技大学考试试题纸（ A 卷）

（ 2020 － 2021 学年度第 1 学期）

课程名称: 信息安全管理 开课单位: 计算机学院 命题教师: 李章兵

授课对象: 计算机 学院 17 年级 信安 1-3 班

考试时量: 100 分钟 考核方式: 考试 考试方式: 闭卷

审核人: 审核时间: 年 月 日

一、判断题 (本题共 20 分, 每小题 2 分)

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。（ ）

2. 信息安全策略的制定和维护中，最重要的是要保证其明确性和相对稳定性。（ ）

3. 信息安全评测系统 CC 是国内标准。 （ ）

4. 采用渗透性测试来检测系统安全脆弱性，是安全评估过程中的常用手段。 ( )

5. “资产责任人”是指有权限变更资产安全属性的人。( )

6. 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。（ ）

7. 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。（ ）

8. 进行信息安全管理教育和培训，可以有效解决人员安全意识薄弱。（ ）

9.《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。（ ）

10. 安全审计跟踪是审计安全事件并追踪系统安全检测的过程。（ ）

二、选择题 (本题共 30 分, 每小题 2 分，必要时多选)。

1. 信息安全经历了三个发展阶段，以下( )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. 信息安全管理领域权威的标准是（ ）。
A. ISO 15408 B. ISO 17799/ISO 27001(英） C. ISO 9001 D. ISO 14001

3. 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

4. 信息安全管理体系是 PDCA 动态持续改进的一个循环体。下面理解不正确的是（ ）。

A. 推动 PDCA 循环，关键在 P 这个计划阶段。
B. 组织中的每个部分或个人，均可以 PDCA 循环，大环套小环，一层一层地解决问题。
C. 每通过一次 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环。
D. 按顺序进行，它靠组织的力量来推动，像车轮一样向前进，周而复始，不断循环。

5. 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

6. 涉及国家秘密的计算机信息系统，必须 (　　) 。
A. 实行逻辑隔离　B. 实行单向隔离　C. 实行物理隔离　D. 以上都不是

7. 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. 蓄电池　B. 发电机　C. 干电池　D. UPS

8. 区域安全管理中下面哪个描述是错误的？（　　）
A. 安全区域保护可采用围墙和门控，警卫、智能锁、电子监视和警报系统都是适当措施。
B. 隔离送货区域、装载区域、信息处理设施，控制授权访问。
C. 敏感信息处理设施的位置标示引人注目，安装监控。
D. 来访人员进入需要审批并记录。

9. 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

10. 对于信息安全管理中的人力资源安全，以下理解不正确的是（　　）。
A. 上岗前要对担任敏感和重要岗位的人员要考察其以往的违法违规记录
B. 雇佣中要有及时有效的惩戒措施
C. 出了事故后要有针对性地进行信息安全意识教育和技能培训
D. 离职人员要撤销其访问权限

11. 信息安全的符合性检查不包括（　　）
A. 法律法规符合性　B. 技术标准符合性
C. 安全策略符合性　D. 内部审核活动

12. 信息安全领域内最关键和最薄弱的环节是（　　）。
A. 技术　B. 策略　C. 管理制度　D. 人

13. 业务连续性管理 (BCM) 的原则是预防为先，恢复为后，其中预防的目的是(　　)。
A. 减少威胁的可能性　B. 保护企业的弱点区域
C. 减少灾难发生的可能性　D. 防御危险的发生并降低其影响

14. 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. 发布管理　B. IT 服务持续性管理　C. 问题管理　D. 变更管理

15. 1999 年我国发布的信息安全等级保护国家标准 GB 17859-1999 考了美国的 TCSEC 标准，将信息系统的安全等级划分为（　　）个等级。

A. 7　B. 6　C. 5　D. 4

三、问答题 (本题共 40 分, 每小题 10 分)。

1. 什么是信息安全管理体系 ISMS？建立 ISMS 分哪几步骤？（10’）
2. ISO27001 所关注的 11 大领域是什么？（10’）
3. 简述信息安全风险的七大要素，并画图说明要素之间的相互关系。（10’）
4. 信息系统生命周期包括哪 5 个阶段？信息系统安全等级分哪几级？与系统生命周期对应的安全等级保护实施过程是什么？（10’）

四、综合分析题 (本题共 10 分)。

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。请从信息安全管理上分析。

附加题：（10 分）

请就手机 APP 的下载、安装和使用过程，以及共享充电、公共 WIFI 的使用谈谈如何进行信息安全管理。

湖南科技大学考试试题参考答案及评分细则

（2020-2021 学年度第 1 学期）

课程（A 卷） 信息安全管理 **上课学院** 计算机学院 **班级** 2017 级信息安全 1-3 班

应试学生人数 97 **实际考试学生人数** _____ **考试时量** 100 **分钟**

命题教师 李章兵 **审核人** _____ **考试时间：** 年 月 日

一、判断题 (本题共 20 分, 每小题 2 分)

1-5 ×√×√√ 6-10 √√√√×

二、单项选择题 (本题共 30 分, 每小题 2 分)。

1-5 BBBAD 6-10 CDCAB 11-15 DDCAC

三、简答题 (本题共 20 分, 每小题 10 分)

1. 参考答案：信息安全管理体系（Information Security Management System，ISMS）是组织在整体或特定范围内建立的信息安全方针和目标，以及完整这些目标所用的方法和手段所构成的体系。

   建立 ISMS 的步骤：1-信息安全管理体系的策划与准备；2-信息安全管理体系文件的编制；3-建立信息安全管理框架；4-信息安全管理体系的运行；5-信息安全管理体系的审核与评审。

2. 参考答案：信息安全 11 大管理领域：

   安全方针/策略、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、信息系统开发与维护、信息安全事件管理、业务连续性管理、法律法规符合性。

3. 参考答案：信息安全风险的七大要素：资产、威胁、脆弱点、风险、影响、安全措施和安全需求。

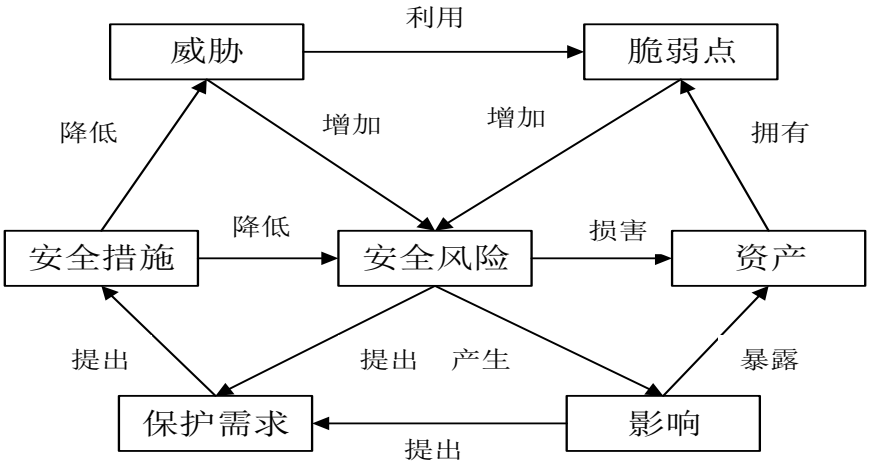
   资产：是任何对组织有价值的东西；

   威胁：可能导致信息安全事故和组织信息资产损失的活动，是利用脆弱性造成的后果；

   脆弱性：与信息资产有关的弱点或安全隐患，本身并不对资产构成危害，但是在一定条件得到满足时，会被威胁利用来危害信息资产；

   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。



4. 参考答案：

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。

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。

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。与信息系统生命周期对应的等级保护实施过程有 5 步：系统定级、安全规则、安全实施、安全运行维护和系统终止。

四、综合分析题 (本题共 10 分)

参考答案主要观点：

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。

1. 笔记本带出办公室，有丢失、被非法访问风险；采取随身锁的安全措施；
2. 在家里使用，有感染病毒、泄露单位重要文件信息的风险；采取隔离家庭网络或防火墙、杀毒防护措施；
3. 染毒的笔记本带回办公室，有交叉感染办公室台式电脑的风险，有交叉拷贝数据文件被泄露的风险；采取严格的杀毒与隔离措施。
4. 如果工作有较高等级涉密信息，严禁将电脑带出办公室，并严管 U 盘使用，避免“摆渡”APT 攻击。
5. 定期对单位进行信息安全管理培训，增强领导和员工的信息安全意识。

附加题（10 分）

自由发挥，酌情加分。