湖南科技大学考试试题纸（ A 卷）

（ 2022 － 2023 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 19 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。（ ）

2. 安全风险评估过程中由于参数确定较为困难，实际往往多采取定性评估，或者定性和定量评估相结合的方法。 ( )

3. ISO17799 的合规性定义除了符合法律要求、安全策略和技术规范检查，还包括系统审查相关事项。 （ ）

4. “资产责任人”是指有权限变更资产安全属性的人。( )

5. 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。（ ）

6. 安全事件监控是指基于合规性或审计目的来跟踪和记录安全数据，实时监控和分析安全事件的发生和可能。（ ）

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. 信息安全领域内最关键和最薄弱的环节是安全技术（ ）

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、单项选择题 (本题共 30 分, 每小题 2 分)

1. 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

2. 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

3. 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。

4. 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

5. 人员安全管理原则不包括 (　　) 。
A. 多人负责　B. 任期有限　C. 授权管理　D. 职责分离

6. 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

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. 下面哪个是组织的信息资产？（　　）
A. 家具　B. 场地　C. 电子邮件　D. 都是

10. 下面哪个不是信息资产的保护措施？（　　）
A. 编制资产清单　B. 分类标记　C. 指定责任人　D. 清查盘点

11. 英国 ITIL 的核心模块是服务管理，下面哪个不属于服务提供管理流程？（　　）
A. 服务级别管理　B. 可用性管理　C. 发布管理　D. 服务财务管理

12. 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

13. ITIL 安全事件监控的主要工作不包括（　　）
A. 日志审计　B. 关联分析　C. 安全事件知识库　D.建立统一管理平台

14. 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

15. 安全审计流程不包括（　　）

A. 事件采集　**B.** 事件分析　**C.** 事件监控　**D.** 事件响应

三、问答题 **(**本题共 **50** 分**)**。

1. 什么是信息安全管理体系 **ISMS**？建立 **ISMS** 分哪几步骤？（**8’**）

2. 什么是详细风险评估？画出其流程图并说明（**15’**）

3. 信息系统安全等保测评的目的是什么？如何确定其安全等级？试画出安全等级矩阵表。**(12’**）

4.试画图说明等级保护的基本安全要求和等级保护的完全实施流程。**(15** 分**)**

附加题：（**10** 分）

请就手机的使用谈谈如何进行信息安全管理。（如：**APP** 的下载、安装和使用过程，以及共享充电、公共 **WIFI**、防窃听窃照）